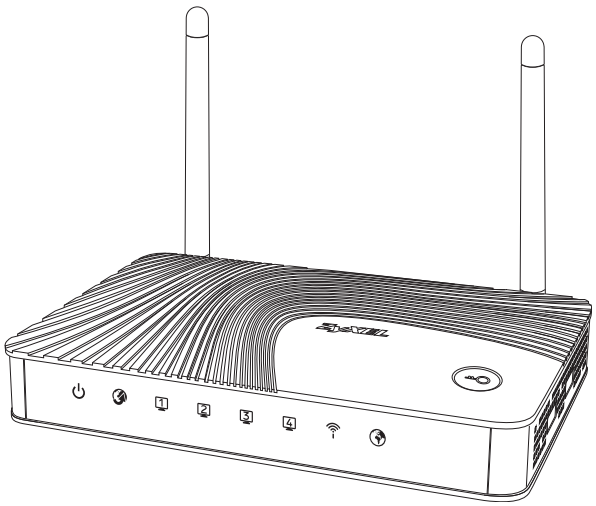
EMG1302-R10A

Wireless N300 4-port Ethernet Gateway

Version V1.00
Edition 1, 1/2014



User's Guide

Default Login Details	
LAN IP Address	http://192.168.1.1
User Name	supervisor
Password	supervisor
User Name	admin
Password	1234

Copyright © 2013 ZyXEL Communications Corporation

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Note: This guide is a reference for a series of products. Therefore some features or options in this guide may not be available in your product.

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the EMG1302-R10A and access the Web Configurator. It contains information on setting up your wireless network.

Contents Overview

User's Guide 11

Introduction 13
Introducing the Web Configurator 17
Quick Start 21
Monitor 27
Router Mode 33
Tutorials 41

Technical Reference 51

WAN 53
Wireless LAN 73
LAN 91
DHCP Server 95
Quality of Service (QoS) 101
NAT 107
DDNS 115
Routing 117
Interface Group 121
Security 123
Content Filtering 129
IPv6 Firewall 133
Remote Management 135
Universal Plug-and-Play (UPnP) 143
Maintenance 151
Troubleshooting 159

Table of Contents

Contents Overview 3

Table of Contents 5

Part I: User's Guide 11

Chapter 1
Introduction 13

1.1 Overview 13
1.2 Applications 13
1.3 Ways to Manage the EMG1302-R10A 13
1.4 Good Habits for Managing the EMG1302-R10A 13
1.5 LEDs 14
1.6 The WPS Button 15
1.7 Wall Mounting 16

Chapter 2
Introducing the Web Configurator 17

2.1 Overview 17
2.2 Login Accounts 17
2.3 Accessing the Web Configurator 17
2.4 Resetting the EMG1302-R10A 19
2.4.1 Procedure to Use the RESET Button 19

Chapter 3
Quick Start 21

3.1 Overview 21
3.2 Quick Start Setup 21

Chapter 4
Monitor 27

4.1 Overview 27
4.2 What You Can Do 27
4.3 The Log Screen 28
4.3.1 View Log 28
4.3.2 Log Setting 29
4.4 DHCP Table 29
4.5 Packet Statistics 30

4.6 WLAN Station Status 31

Chapter 5
Router Mode 33

5.1 Overview 33
5.2 Router Mode Status Screen 34
5.2.1 Navigation Panel 37

Chapter 6
Tutorials 41

6.1 Overview 41
6.2 Set Up a Wireless Network with WPS 41
6.2.1 Push Button Configuration (PBC) 41
6.2.2 PIN Configuration 42
6.3 Configure Wireless Security without WPS 43
6.3.1 Configure Your Notebook 45
6.4 Using Multiple SSIDs on the EMG1302-R10A 47
6.4.1 Configuring Security Settings of Multiple SSIDs 48

Part II: Technical Reference 51

Chapter 7
WAN 53

7.1 Overview 53
7.2 What You Can Do 53
7.3 What You Need To Know 54
7.3.1 Configuring Your Internet Connection 54
7.3.2 Multicast 55
7.4 Management WAN 57
7.4.1 Add/Edit Internet Connection 58
7.4.2 Bridge Encapsulation 69
7.5 Advanced WAN Screen 70
7.6 IPv6 Screen 71

Chapter 8
Wireless LAN 73

8.1 Overview 73
8.2 What You Can Do 73
8.3 What You Should Know 74
8.4 General Wireless LAN Screen 76
8.5 Wireless Security 79

8.5.1 No Security 79
8.5.2 WPA2-PSK 80
8.6 More AP 81
8.6.1 More AP Edit 82
8.7 MAC Filter 83
8.8 Wireless LAN Advanced Screen 84
8.9 Quality of Service (QoS) Screen 85
8.10 WPS Screen 86
8.11 WPS Station Screen 87
8.12 Scheduling Screen 88
8.13 WDS 89

Chapter 9
LAN 91

9.1 Overview 91
9.2 What You Can Do 91
9.3 What You Need To Know 92
9.3.1 IP Pool Setup 92
9.3.2 LAN TCP/IP 92
9.4 LAN IP Screen 93

Chapter 10
DHCP Server 95

10.1 Overview 95
10.2 What You Can Do 95
10.3 What You Need To Know 95
10.4 The DHCP General Screen 96
10.5 The DHCP Advanced Screen 97
10.6 The DHCP Client List Screen 98

Chapter 11
Quality of Service (QoS) 101

11.1 Overview 101
11.1.1 What You Can Do in the QoS Screens 102
11.1.2 What You Need to Know About QoS 102
11.2 The Quality of Service General Screen 102
11.3 The Rule-based QoS Screen 103
11.3.1 Adding a Rule 104
11.4 QoS Technical Reference 105
11.4.1 IEEE 802.1p 105
11.4.2 IP Precedence 105
11.4.3 Automatic Priority Queue Assignment 105

Chapter 12
NAT 107

12.1 Overview 107
12.2 What You Can Do 107
12.3 What You Need To Know 108
12.4 The NAT General Screen 110
12.5 The NAT Port Forwarding Screen 110
12.6 The NAT Trigger Port Screen 111
12.7 The ALG Screen 113

Chapter 13
DDNS 115

13.1 Overview 115
13.2 The DDNS General Screen 115

Chapter 14
Routing 117

14.1 Overview 117
14.2 Static Route Screen 117
14.2.1 Add/Edit Static Route Screen 118
14.3 The Dynamic Routing Screen 119

Chapter 15
Interface Group 121

15.1 Overview 121
15.2 The Interface Group Screen 121
15.2.1 Add Interface Group 122

Chapter 16
Security 123

16.1 Overview 123
16.2 What You Can Do 123
16.3 What You Need To Know 124
16.4 The Firewall General Screen 125
16.5 The Firewall Services Screen 126

Chapter 17
Content Filtering 129

17.1 Overview 129
17.2 What You Need To Know 129
17.3 Content Filter 130

Chapter 18
IPv6 Firewall 133

18.1 Overview 133
18.2 The IPv6 Firewall Screen 133

Chapter 19
Remote Management 135

19.1 Overview 135
19.2 What You Need to Know 135
19.2.1 Remote Management and NAT 135
19.3 What You Can Do 135
19.4 The WWW Screen 136
19.5 The Telnet Screen 137
19.6 The SNMP Screen 138
19.7 The TR069 Screen 140

Chapter 20
Universal Plug-and-Play (UPnP) 143

20.1 Overview 143
20.2 What You Need to Know 143
20.2.1 NAT Traversal 143
20.2.2 Cautions with UPnP 143
20.3 UPnP Screen 144
20.4 Technical Reference 144
20.4.1 Using UPnP in Windows XP Example 144
20.4.2 Web Configurator Easy Access 147

Chapter 21
Maintenance 151

21.1 Overview 151
21.2 What You Can Do 151
21.3 General Screen 151
21.4 Account Screen 152
21.4.1 Account Setup Screen 152
21.5 Time Setting Screen 154
21.6 Firmware Upgrade Screen 155
21.7 Configuration Backup/Restore Screen 156
21.8 Restart Screen 158

Chapter 22
Troubleshooting 159

22.1 Overview 159
22.2 Power, Hardware Connections, and LEDs 159

22.3 EMG1302-R10A Access and Login 160
22.4 Internet Access 161
22.5 Resetting the EMG1302-R10A to Its Factory Defaults 162
22.6 Wireless Router/AP Troubleshooting 163

Appendix A Customer Support 166

Appendix B Pop-up Windows, JavaScript and Java Permissions 173

Appendix C Wireless LANs 185

Appendix D Common Services 199

Appendix E Legal Information 203

Index 211

PART I
User's Guide

1 Introduction

1.1 Overview

This chapter introduces the main features and applications of the EMG1302-R10A.

The EMG1302-R10A Wireless N300 4-port Ethernet Gateway is an Ethernet Gateway that provides four Ethernet ports meeting the IEEE 802.11 b/g/n wireless standard, and it features TR-069 remote management for telcos, service providers and cable operators as a home network solution interoperating an FTTx or cable infrastructure.

A range of services such as a firewall and content filtering are also available for secure Internet computing.

1.2 Applications

Your can create the following networks using the EMG1302-R10A:

- **Wired**. You can connect network devices via the Ethernet ports of the EMG1302-R10A so that they can communicate with each other and access the Internet.
- **Wireless**. Wireless clients can connect to the EMG1302-R10A to access network resources.
  - **WPS**. Create an instant network connection with another WPS-compatible device, sharing your network connection with it.
- **WAN**. Connect to a broadband modem/router for Internet access.

1.3 Ways to Manage the EMG1302-R10A

Use any of the following methods to manage the EMG1302-R10A.

- WPS (Wi-Fi Protected Setup). You can use the WPS button or the WPS section of the Web Configurator to set up a wireless network with your ZyXEL Device.
- Web Configurator. This is recommended for everyday management of the EMG1302-R10A using a (supported) web browser.

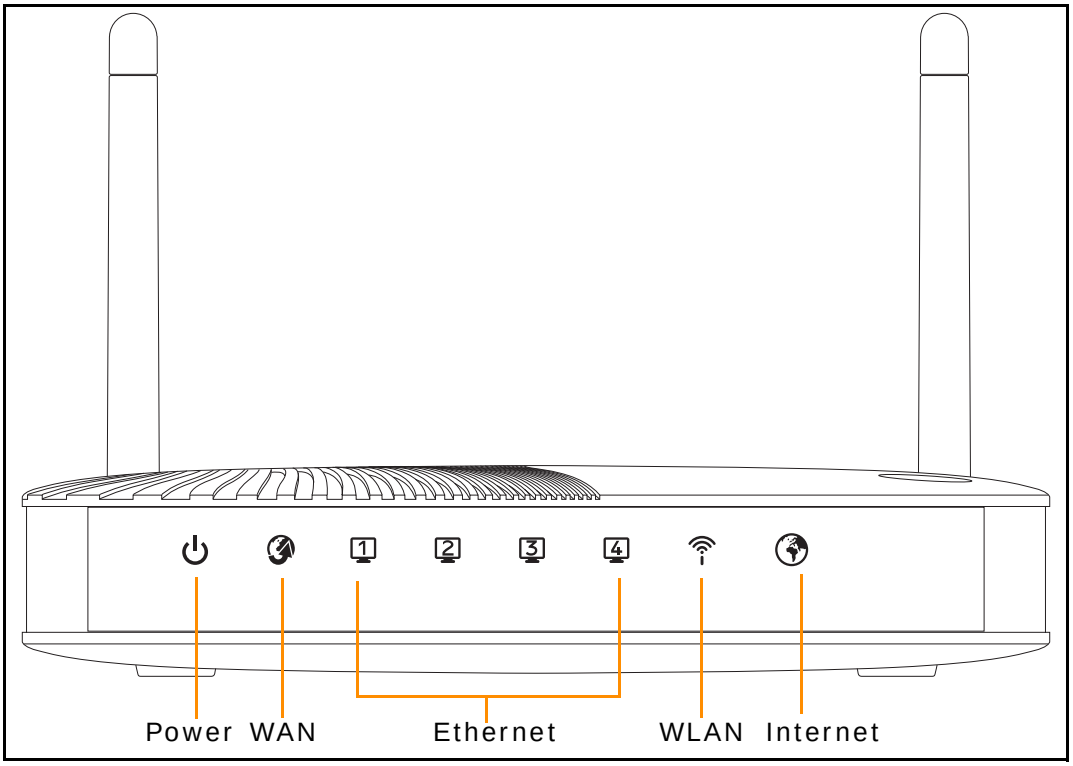
1.4 Good Habits for Managing the EMG1302-R10A

Do the following things regularly to make the EMG1302-R10A more secure and to manage the EMG1302-R10A more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the EMG1302-R10A to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the EMG1302-R10A. You could simply restore your last configuration.

1.5 LEDs

Figure 1 Front Panel



The following table describes the LEDs.

Table 1 Front panel LEDs

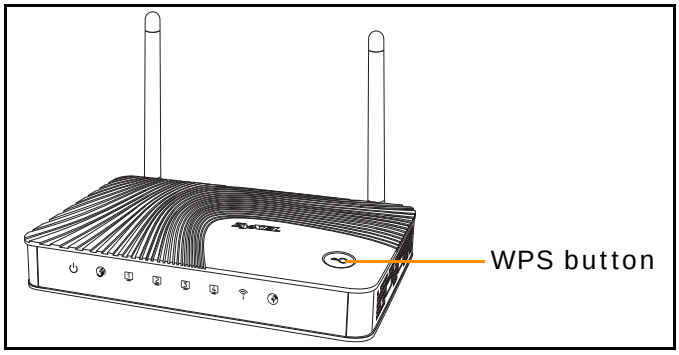
LED	COLOR	STATUS	DESCRIPTION
Power	Green	On	The EMG1302-R10A is receiving power and functioning properly.
	Off		The EMG1302-R10A is not receiving power.
WAN	Green	On	The EMG1302-R10A's WAN connection is ready.
		Blinking	The EMG1302-R10A is sending/receiving data through the WAN with a 10/100Mbps transmission rate.
	Off		The WAN connection is not ready, or has failed.

Table 1 Front panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
LAN 1-4	Green	On	The EMG1302-R10A's LAN connection is ready.
		Blinking	The EMG1302-R10A is sending/receiving data through the LAN with a 10/100Mbps transmission rate.
	Off		The LAN connection is not ready, or has failed.
WLAN	Green	On	The EMG1302-R10A is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The EMG1302-R10A is sending/receiving data through the wireless LAN.
	Off		The wireless LAN is not ready or has failed.
Internet	Green	On	Internet (WAN) connection is up (e.g. PPPeE/DHCP Client).
		Blinking	Internet connection established.
	Off		Internet connection is down.

1.6 The WPS Button

Figure 2 Front Panel



Your EMG1302-R10A supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

For more information on using WPS, see Section 6.2 on page 41.

1.7 Wall Mounting

You may need screw anchors if mounting on a concrete or brick wall.

Table 2 Wall Mounting Information

Distance between holes (measured from center to center)	10.25 cm
M4 Screws	Two
Screw anchors (optional)	Two

1 Select a position free of obstructions on a wall strong enough to hold the weight of the device.

2 Mark two holes on the wall at the appropriate distance apart for the screws.

Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

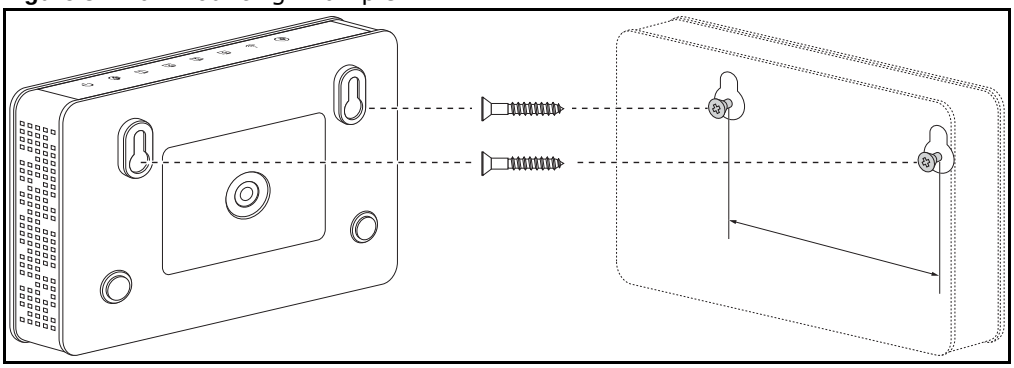
3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.

If not using screw anchors, use a screwdriver to insert the screws into the wall. Do not insert the screws all the way in - leave a gap of about 0.5 cm.

4 Make sure the screws are fastened well enough to hold the weight of the EMG1302-R10A with the connection cables.

5 Align the holes on the back of the EMG1302-R10A with the screws on the wall. Hang the EMG1302-R10A on the screws.

Figure 3 Wall Mounting Example



2

Introducing the Web Configurator

2.1 Overview

This chapter describes how to access the EMG1302-R10A Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy setup and management of the EMG1302-R10A via Internet browser. Use Internet Explorer 6.0 and later versions, Mozilla Firefox 3 and later versions, or Safari 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Refer to the Troubleshooting chapter (Chapter 22 on page 159) to see how to make sure these functions are allowed in Internet Explorer.

2.2 Login Accounts

There are two system accounts that you can use to log in to the EMG1302-R10A: "**admin**" and "**supervisor**". These two accounts have different privilege levels. The web configurator screens vary depending on which account you use to log in.

The **supervisor** accounts allows you full access to all system configurations. The default supervisor user name is "supervisor" and password is "supervisor".

With the **admin** account, you cannot access **Remote MGMT**. The default username is "admin" and password is "1234".

2.3 Accessing the Web Configurator

1. Make sure your EMG1302-R10A hardware is properly connected and prepare your computer or computer network to connect to the EMG1302-R10A (refer to the Quick Start Guide).
2. Launch your web browser.

3 Type "http://192.168.1.1" as the website address.

Your computer must be in the same subnet in order to access this website address.

4 If you are logging in with the "**admin**" account, type "1234" (default) as the password.
If you are logging in with the "**supervisor**" account, type "supervisor" (default) as the password.
Then click **Login**.

Figure 4 Admin Account Login

ZyXEL
EMG1302-R10A
Welcome to the configuration interface. Please enter username and password to login.
User :
Password :
Login
(max. 30 alphanumeric, printable characters and no spaces)

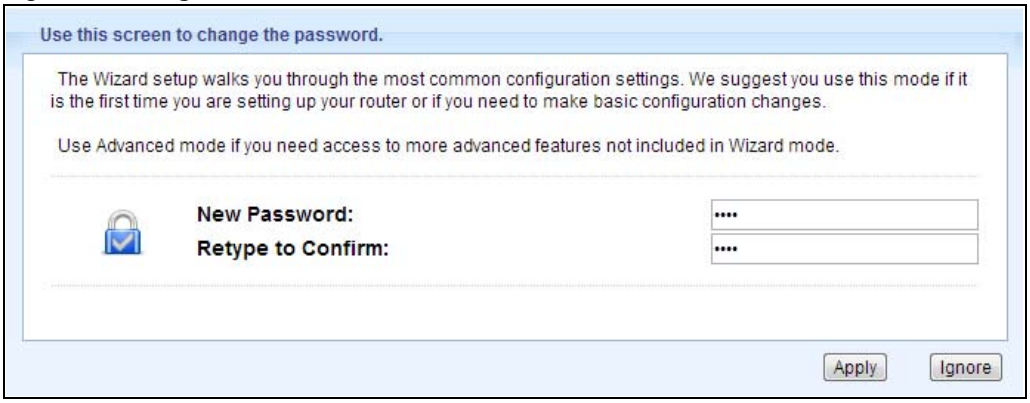
The following table describes the labels in this screen.

Table 3 Login screen

LABEL	DESCRIPTION
User Name	Type "admin" or "supervisor" as the user name.
Password	Type "1234" (default) as the password.
Login	Click **Login** to enter the EMG1302-R10A's web configurator.

5 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Figure 5 Change Password Screen


Use this screen to change the password.
The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.
Use Advanced mode if you need access to more advanced features not included in Wizard mode.
New Password:
Retype to Confirm:
Apply
Ignore

The following table describes the labels in this screen.

Table 4 Change Password Screen

LABEL	DESCRIPTION
New Password	Type a new password.
Retype to Confirm	Retype the password for confirmation.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Ignore	Click **Ignore** if you do not want to change the password this time.

Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes; go to Chapter 21 on page 151 to change this). Simply log back into the EMG1302-R10A if this happens.

2.4 Resetting the EMG1302-R10A

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the **RESET** button at the back of the EMG1302-R10A to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to "supervisor" and the IP address will be reset to "192.168.1.1".

2.4.1 Procedure to Use the RESET Button

1. Make sure the power LED is on.
2. Press and hold the **RESET** button for at least 1 second to restart/reboot the EMG1302-R10A.
3. Press and hold the **RESET** button for at least 5 seconds to set the EMG1302-R10A back to its factory-default configurations.

3

Quick Start

3.1 Overview

Use the Quick Start screens to configure the ZyXEL Device's time zone and basic Internet access and wireless settings.

Note: See the technical reference chapters (starting on page 55) for background information on the features in this chapter.

3.2 Quick Start Setup

1 Click the **Wizard** icon in the top right corner of the web configurator to open the quick start screens. Select the time zone of the ZyXEL Device's location and click **Next**.

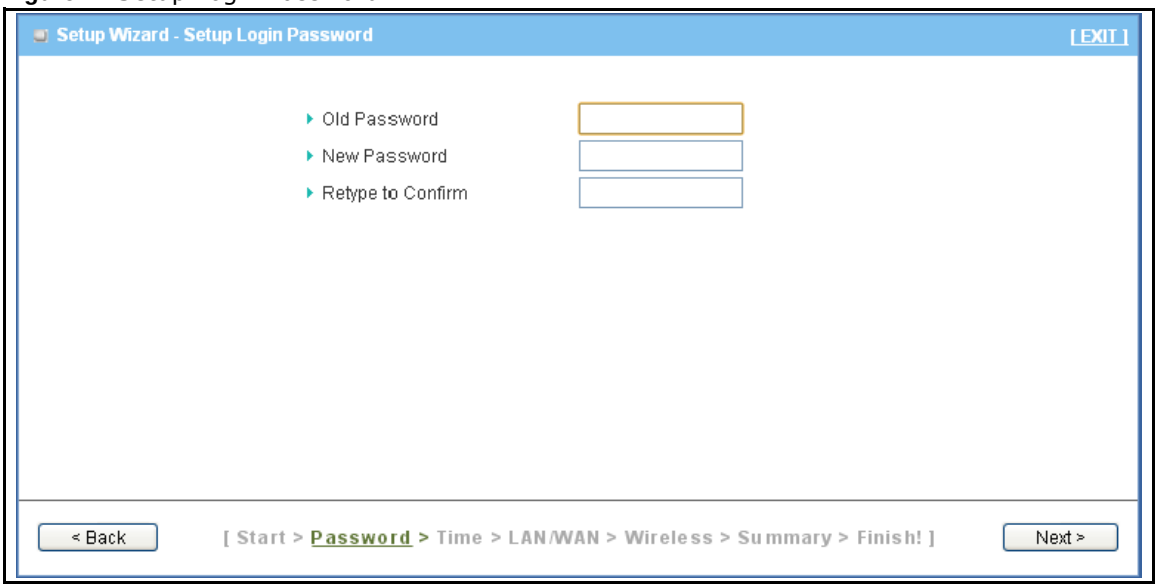
Figure 6 Time Zone

Setup Wizard
[EXIT]
Setup Wizard will guide you through a basic configuration procedure step by step.
Step 1. Setup Login Password.
Step 2. Setup Time Zone.
Step 3. WAN Setup.
Step 4. Wireless Setup.
Step 5. Summary.
Step 6. Finish.
< Back
[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]
Next >

2 To change the current password, enter your existing password in the **Old Password field** and the new password in the **New Password** and **Retype to Confirm** fields.

3 Click **Next** to continue.

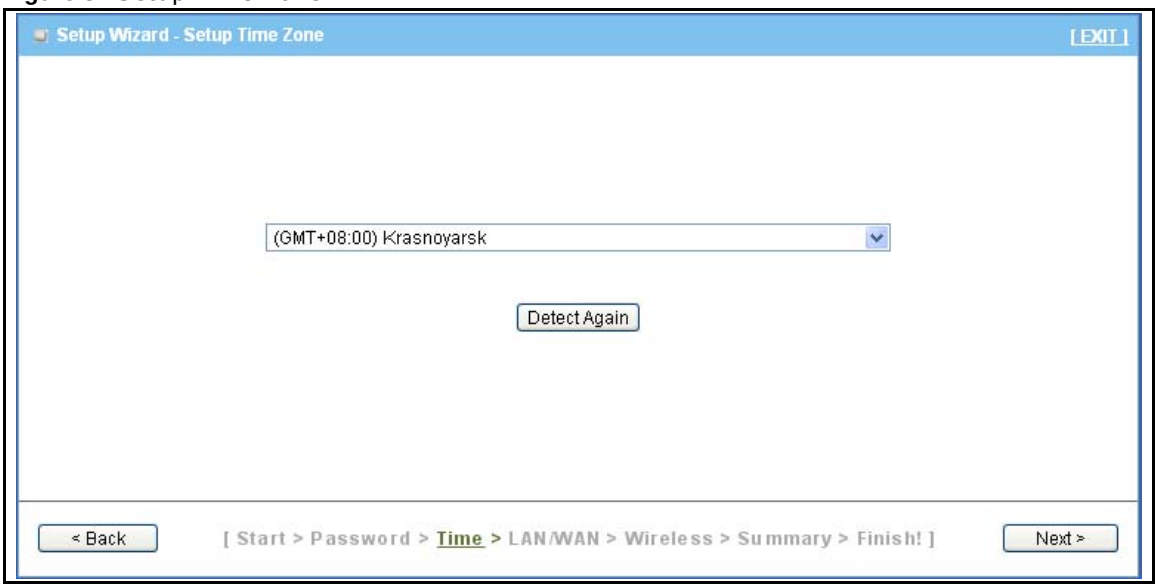
Figure 7 Setup Login Password


Setup Wizard - Setup Login Password
[EXIT]
Old Password
New Password
Retype to Confirm
< Back
[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]
Next >

4 Select the time zone for this device from the drop-down menu or click **Detect Again** to automatically select the time zone.

5 Click **Next** to continue.

Figure 8 Setup Time Zone


Setup Wizard - Setup Time Zone
[EXIT]
(GMT+08:00) Krasnoyarsk
Detect Again
< Back
[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]
Next >

6 Setup the WAN type by selecting a configuration type from the **WAN Type** drop-down menu.

7 Enter the device's IP address in the **LAN IP Address** field if a static IP address is assigned.

8 Click **Next** to continue.

Figure 9 Select WAN Type

Setup Wizard - Select WAN Type
[EXIT]
LAN IP Address
192.168.1.156
WAN Type
Dynamic IP Address
< Back
[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]
Next >

9 Configure the WAN type, select from the following settings:

- Dynamic IP Address (default)
- Static IP Address
- PPP Over Ethernet
- PPTP

10 The WAN Type window as selected above displays. Fill in the respective fields to complete the WAN Type configuration.

11 Click **Next** to continue.

Figure 10 Configure Dynamic IP Address

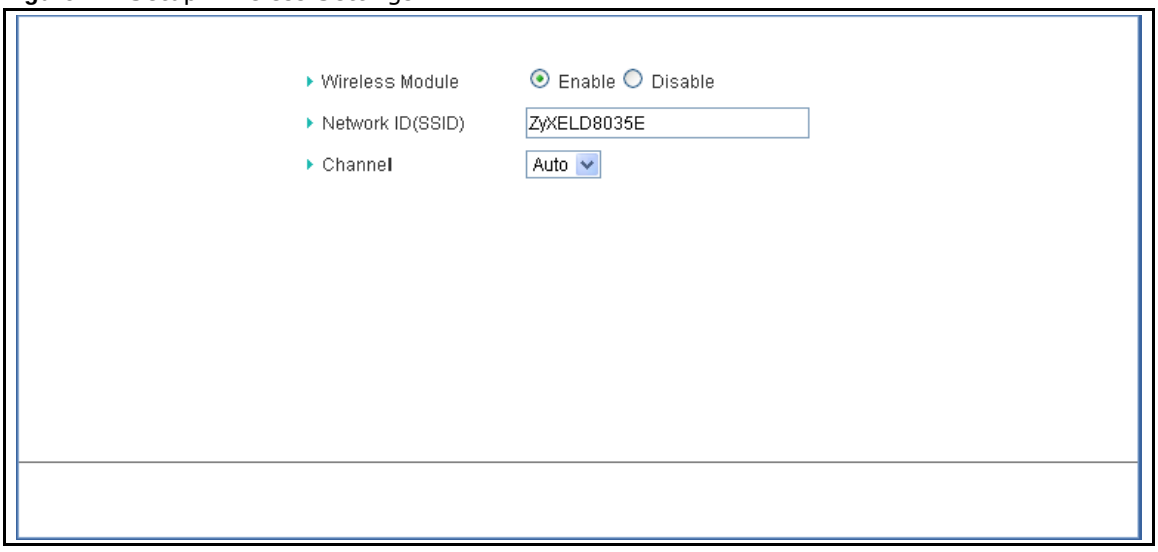
12 In the Wireless settings menu, select **Enable** to activate the device's wireless function.

13 Enter the SSID in the Network ID field to identify this device on the network.

14 Select a channel designation from the drop-down menu or select **Auto** to allow the device to automatically assign one.

15 Click **Next** to continue.

Figure 11 Setup Wireless Settings



16 Select a security mode from the drop-down menu: **WPA2-PSK** (default) or **No Security**.

17 Enter a pre-shared key or use the automatically generated key in the **Pre-Shared Key** field.

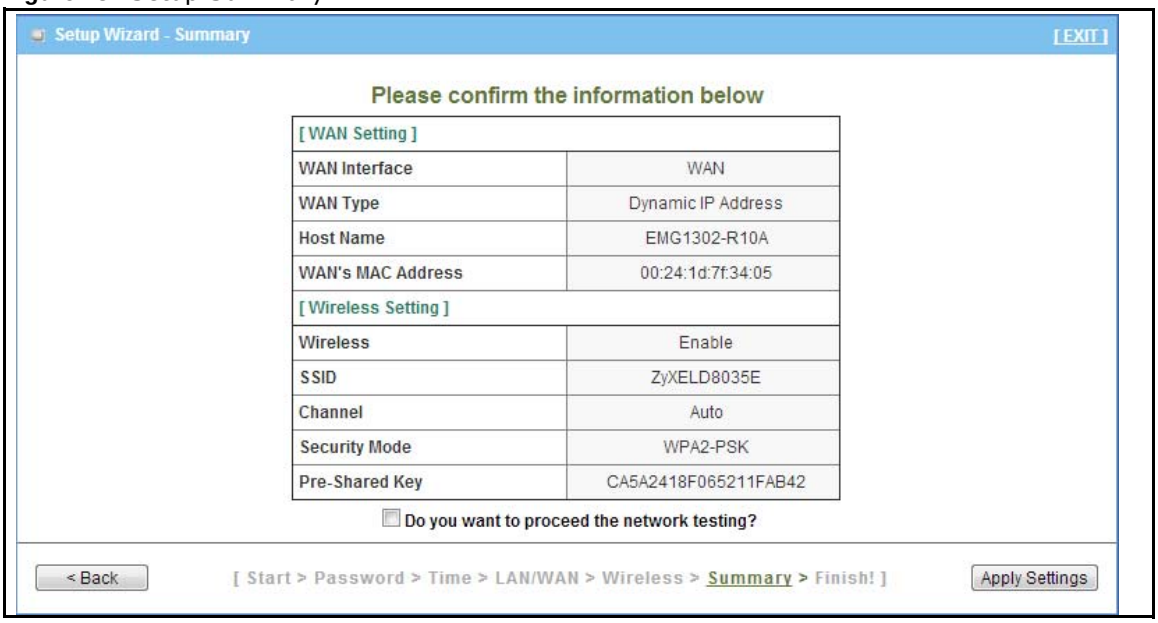
18 Click **Next** to continue.

Figure 12 Setup Wireless Security Settings

The Summary window displays with the selected configuration settings.

19 If the information does not require modification, select the **Do you want to proceed the network testing?** and click **Apply Settings**.

Figure 13 Setup Summary



The device begins applying the new settings. The process requires a short time to fully complete.

20 Once the process is complete, click the **Finish** button to return to the **Status** page.

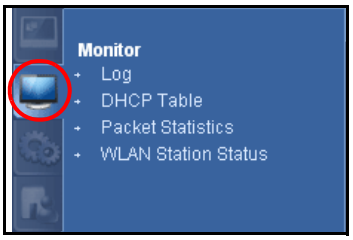
4

Monitor

4.1 Overview

This chapter discusses read-only information related to the device state of the EMG1302-R10A.

To access the Monitor screens, click . Click **open all** to show the complete menu.



You can also click the links in the **Summary** table of the **Status** screen to view the bandwidth consumed, packets sent/received as well as the status of clients connected to the EMG1302-R10A.

4.2 What You Can Do

- Use the **Log** screen to see the logs for the activity on the EMG1302-R10A (Section 4.3 on page 28).
- Use the **DHCP Table** screen to view information related to your DHCP status (Section 4.4 on page 29).
- Use the **Packet Statistics** screen to view port statistics and the "system up time" (Section 4.5 on page 30).
- Use the **WLAN Station Status** screen to view the wireless stations that are currently associated to the EMG1302-R10A (Section 4.6 on page 31).

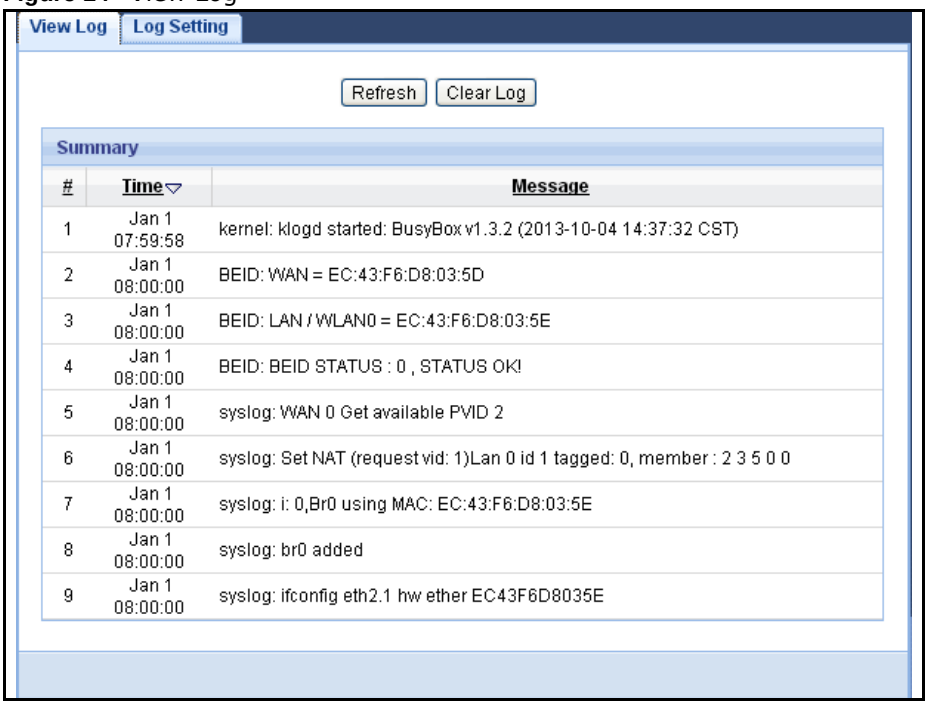
4.3 The Log Screen

The Web Configurator allows you to look at all of the EMG1302-R10A's logs in one location.

4.3.1 View Log

Click **Monitor > Log** to open the **View Log** screen. You can see the logged messages for the EMG1302-R10A. The log wraps around and deletes the old entries after it fills. Click **Clear Log** to delete all the logs. Click **Refresh** to renew the log screen.

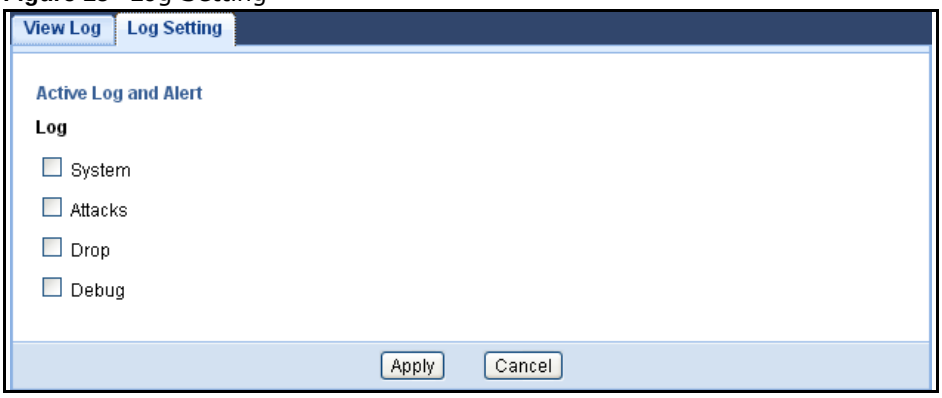
Figure 14 View Log


View Log
Log Setting
Refresh
Clear Log
Summary
Time Message
1 Jan 1 07:59:58 kernel: klogd started: BusyBox v1.3.2 (2013-10-04 14:37:32 CST)
2 Jan 1 08:00:00 BEID: WAN = EC:43:F6:D8:03:5D
3 Jan 1 08:00:00 BEID: LAN / WLAN0 = EC:43:F6:D8:03:5E
4 Jan 1 08:00:00 BEID: BEID STATUS : 0 , STATUS OK!
5 Jan 1 08:00:00 syslog: WAN 0 Get available PVID 2
6 Jan 1 08:00:00 syslog: Set NAT (request vid: 1)Lan 0 id 1 tagged: 0, member : 2 3 5 0 0
7 Jan 1 08:00:00 syslog: i: 0,Br0 using MAC: EC:43:F6:D8:03:5E
8 Jan 1 08:00:00 syslog: br0 added
9 Jan 1 08:00:00 syslog: ifconfig eth2.1 hw ether EC43F6D8035E

4.3.2 Log Setting

You can configure which logs to display in the **View Log** screen. Click **Monitor > Log** to open the **Log Setting** screen and select the logs you wish to display. You can configure active log and alert settings.

Figure 15 Log Setting

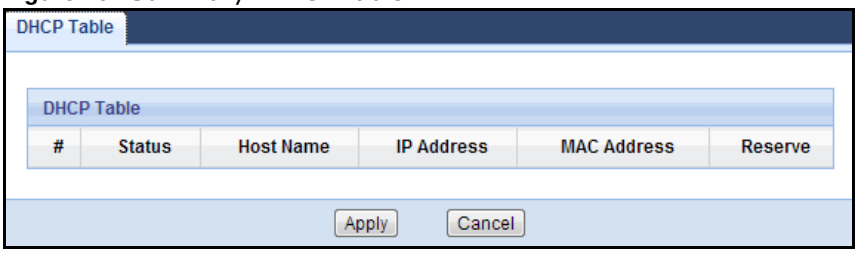


4.4 DHCP Table

Dynamic Host Configuration Protocol (DHCP), RFC 2131 and RFC 2132 allow individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the EMG1302-R10A's LAN as a DHCP server or disable it. When configured as a server, the EMG1302-R10A provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on that network, or else the computer must be manually configured.

Click the **DHCP Table (Details...)** hyperlink in the **Status** screen or **Monitor > DHCP Table**. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **Host Name, IP Address**, and **Mac Address**) of all network clients using the EMG1302-R10A's DHCP server.

Figure 16 Summary: DHCP Table



The following table describes the labels in this screen.

Table 5 Summary: DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
Status	This field displays weather the connection to the host computer is up (a yellow bulb) or down (a grey bulb).
Host Name	This field displays the computer host name.

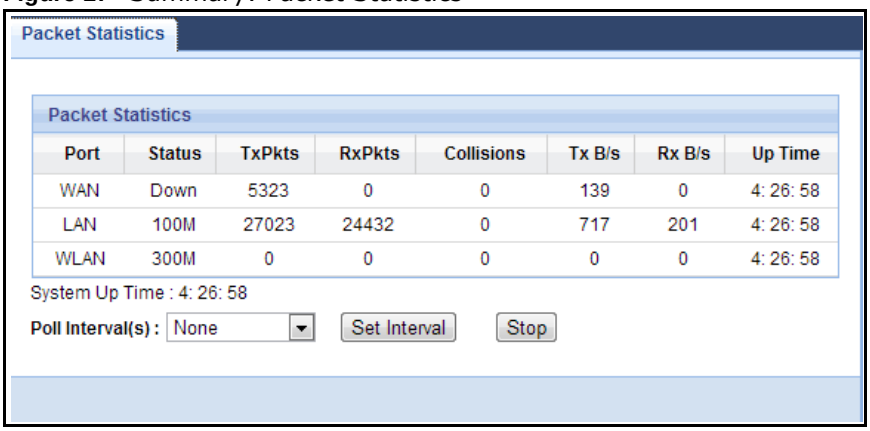
Table 5 Summary: DHCP Table (continued)

LABEL	DESCRIPTION
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	This field shows the MAC address of the computer with the name in the **Host Name** field. Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a device. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Reserve	Select this if you want to reserve the IP address for this specific MAC address.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

4.5 Packet Statistics

Click the **Packet Statistics (Details...)** hyperlink in the **Status** screen or **Monitor > Packet Statistics**. Read-only information here includes port statistics and the "system up time". The **Poll Interval(s)** field is configurable and is used for refreshing the screen.

Figure 17 Summary: Packet Statistics



The following table describes the labels in this screen.

Table 6 Summary: Packet Statistics

LABEL	DESCRIPTION
Port	This is the EMG1302-R10A's port type.
Status	For the LAN ports, this displays the port speed and duplex setting or **Down** when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and Drop (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays Down when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **Down** when the WLAN is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.

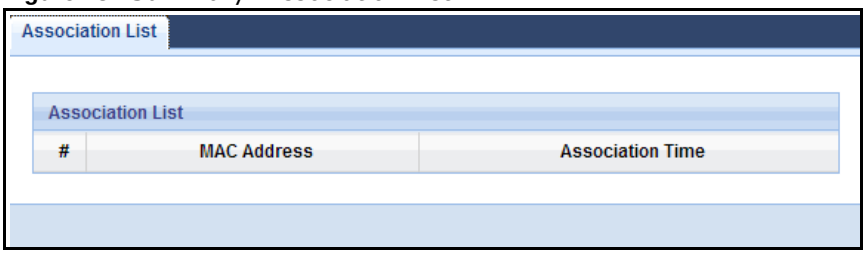
Table 6 Summary: Packet Statistics (continued)

LABEL	DESCRIPTION
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total time the EMG1302-R10A has been for each session.
System Up Time	This is the total time the EMG1302-R10A has been on.
Poll Interval(s)	Enter the time interval in seconds for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics.

4.6 WLAN Station Status

Click the **WLAN Station Status (Details...)** hyperlink in the **Status** screen or **Monitor > WLAN Station Status**. View the wireless stations that are currently associated to the EMG1302-R10A in the **Association List**. Association means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the AP (or wireless router) using the same SSID, channel and security settings.

Figure 18 Summary: Association List



The following table describes the labels in this screen.

Table 7 Summary: Wireless Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the EMG1302-R10A's WLAN network.

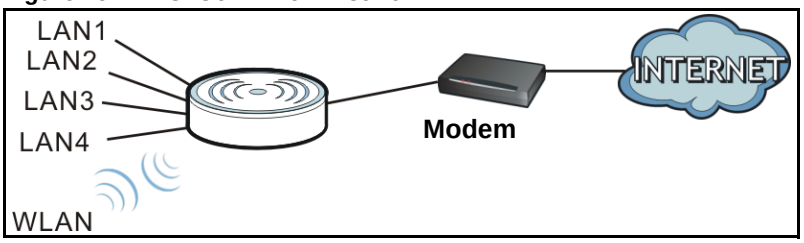
5

Router Mode

5.1 Overview

The EMG1302-R10A router mode connects the local network to another network (for example, the Internet). In the figure below, the EMG1302-R10A connects the local network (**LAN1** ~ **LAN4**) to the Internet.

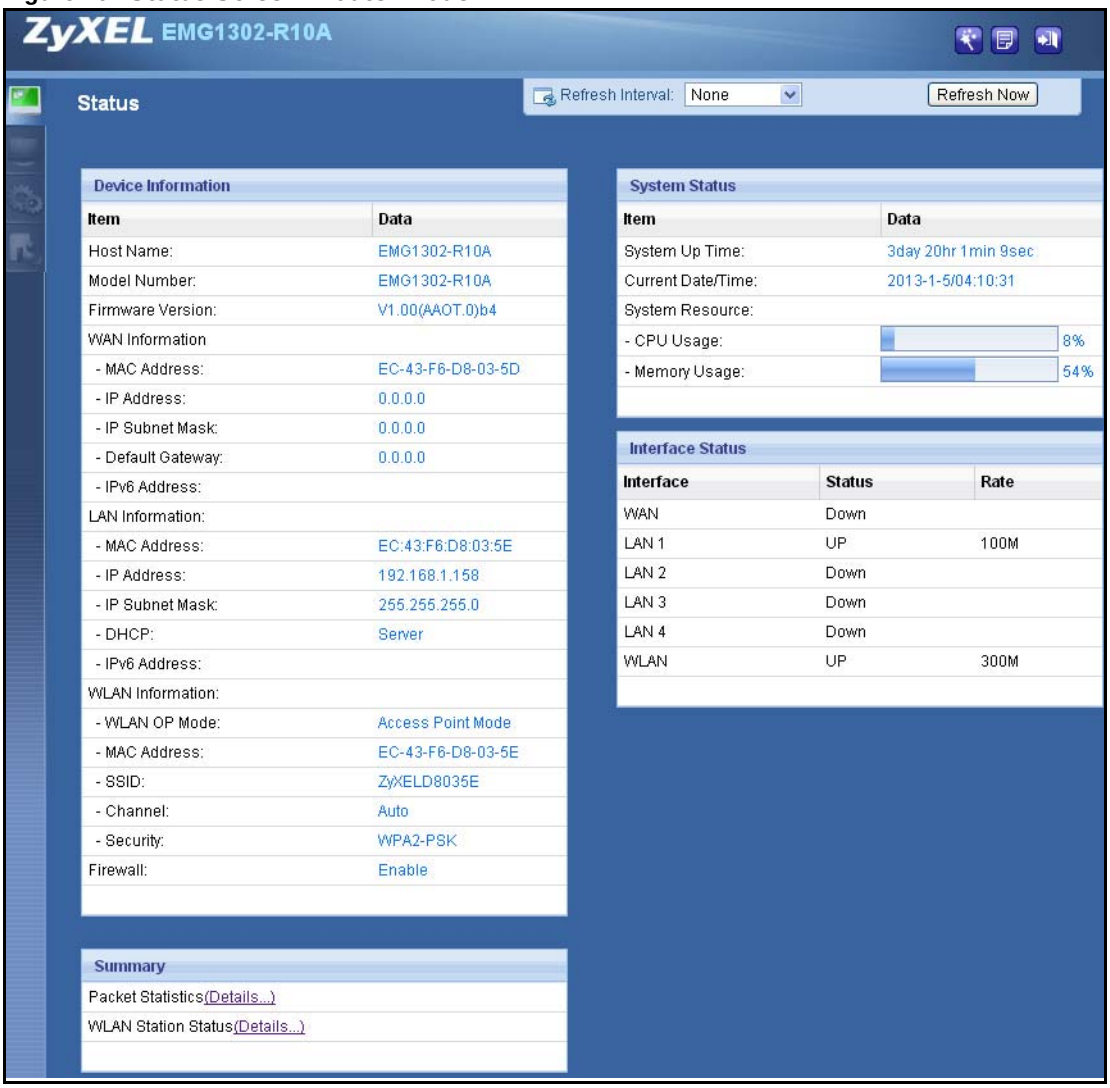
Figure 19 EMG1302-R10A Network



5.2 Router Mode Status Screen

Click to open the status screen.

Figure 20 Status Screen: Router Mode



The following table describes the icons shown in the **Status** screen.

Table 8 Status Screen Icon Key: Router Mode

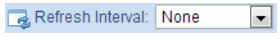
ICON	DESCRIPTION
	Click this icon to open screens where you can configure the ZyXEL Device's time zone Internet access, and wireless settings.
	Click this icon to view copyright and a link for related product information.
	Click this at any time to exit the Web Configurator.
	Select a number of seconds or **None** from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.

Table 8 Status Screen Icon Key: Router Mode (continued)

ICON	DESCRIPTION
Refresh Now	Click this button to refresh the status screen statistics.
	Click this icon to see the **Status** page. The information in this screen depends on the device mode you select.
	Click this icon to see the **Monitor** navigation menu.
	Click this icon to see the **Configuration** navigation menu.
	Click this icon to see the **Maintenance** navigation menu.

The following table describes the labels shown in the **Status** screen.

Table 9 Status Screen: Router Mode

LABEL	DESCRIPTION
Device Information	
Host Name	This is the device's host name.
Model Number	This is the device's model number.
Firmware Version	This is the firmware version.
WAN Information	
- MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the WAN port's IP address.
- IP Subnet Mask	This shows the WAN port's subnet mask.
- Default Gateway	This shows the default gateway address.
- IPv6 Address	This shows the WAN port's IPv6 address.
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows the LAN port's DHCP role - **Server** or **Disable**.
- IPv6 Address	This shows the LAN port's IPv6 address.
WLAN Information	
- WLAN OP Mode	This shows the device mode to which the EMG1302-R10A's wireless LAN is set.
- MAC Address	This shows the wireless adapter MAC Address of your device.
- SSID	This shows a descriptive name used to identify the EMG1302-R10A in the wireless LAN.
- Channel	This shows the channel number which you select manually.
- Security	This shows the level of wireless security the EMG1302-R10A is using.
Firewall	This shows the firewall enabled or not.
System Status	
Item	This column shows the type of data the EMG1302-R10A is recording.
Data	This column shows the actual data recorded by the EMG1302-R10A.
System Up Time	This is the total time the EMG1302-R10A has been on.
Current Date/Time	This field displays your EMG1302-R10A's present date and time.

Table 9 Status Screen: Router Mode (continued)

LABEL	DESCRIPTION
System Resource	
- CPU Usage	This displays what percentage of the EMG1302-R10A's processing ability is currently used. When this percentage is close to 100%, the EMG1302-R10A is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.)
- Memory Usage	This shows what percentage of the heap memory the EMG1302-R10A is using.
Interface Status	
Interface	This displays the EMG1302-R10A port types. The port types are: **WAN**, **LAN** and **WLAN**.
Status	For the LAN and WAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN, it displays **Up** when the WLAN is enabled or **Down** when the WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or **N/A** when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation. This field displays **N/A** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **N/A** when the WLAN is disabled.
WAN	This shows the WAN status and data transfer rate.
LAN1	This shows the LAN1 status and data transfer rate.
LAN2	This shows the LAN2 status and data transfer rate.
LAN3	This shows the LAN3 status and data transfer rate.
LAN4	This shows the LAN4 status and data transfer rate.
WLAN	This shows the WLAN status and data transfer rate.
Summary	
Packet Statistics	Click **Details...** to go to the **Monitor > Packet Statistics** screen (Section 4.5 on page 30). Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click **Details...** to go to the **Monitor > WLAN Station Status** screen (Section 4.6 on page 31). Use this screen to view the wireless stations that are currently associated to the EMG1302-R10A.

5.2.1 Navigation Panel

Use the sub-menus on the navigation panel to configure EMG1302-R10A features.

Figure 21 Navigation Panel: Router Mode

The following table describes the sub-menus.

Table 10 Navigation Panel: Router Mode

LINK	TAB	FUNCTION
Status		This screen shows the EMG1302-R10A's general device, system and interface status information. Use this screen to access the summary statistics tables.
MONITOR		
Log		Use this screen to view the list of activities recorded by your EMG1302-R10A.
DHCP Table		Use this screen to view current DHCP client information.
Packet Statistics		Use this screen to view port status and packet specific statistics.
WLAN Station Status		Use this screen to view the wireless stations that are currently associated to the EMG1302-R10A.
CONFIGURATION		
Open all | close all		Click **Open all** to see all the sub menus in Configuration section. Click **close all** to close all the sub menus in Configuration section.
Network		
WAN	Management WAN	This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers, the WAN MAC address, and VLAN settings.
	Add New WAN Entries	Click to add new ISP parameters for Internet access.

Table 10 Navigation Panel: Router Mode (continued)

LINK	TAB	FUNCTION
Wireless LAN	General	Use this screen to configure wireless LAN and the level of wireless security for the EMG1302-R10A.
	More AP	Use this screen to configure multiple BBs for the EMG1302-R10A.
	MAC Filter	Use the MAC filter screen to configure the EMG1302-R10A to block access to devices or block the devices from accessing the EMG1302-R10A.
	Advanced	This screen allows you to configure advanced wireless settings.
	QoS	Use this screen to enable Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
	WDS	Use this screen to set up Wireless Distribution System links to other access points.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
DHCP Server	General	Use this screen to enable the EMG1302-R10A's DHCP server.
	Advanced	Use this screen to assign IP addresses to specific individual computers based on their MAC addresses and to have DNS servers assigned by the DHCP server.
	Client List	Use this screen to view the individual client list.
QoS	General	Use this screen to enable Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	Rule-based QoS	Use this screen to create traffic policies based on QoS features.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Port Trigger	Use this screen to change EMG1302-R10A port triggering settings.
	ALG	
DDNS	Dynamic DNS	Use this screen to set up dynamic DNS.
Routing	Static Route	Use this screen to configure IP static routes.
	Dynamic Routing	
Interface Group	Interface Group	Use this screen to add a LAN interface or a VLAN ID to a new group.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall and Anti-Dos Attack.
	Services	Use this screen to configure ICMP setting of the EMG1302-R10A.
Content Filter	Content Filter	Use this screen to block sites containing certain keywords in the URL.
IPv6 Firewall	Service	Use this screen to enable (disable) and add IPv6 firewall rules.

Table 10 Navigation Panel: Router Mode (continued)

LINK	TAB	FUNCTION
Management		
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the EMG1302-R10A.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the EMG1302-R10A.
	SNMP	Use this screen to enable Wake on LAN to remotely turn on a device on the local network.
	TR069	Use this screen to configure the remote management over the WAN by an Auto Configuration Server (ACS).
UPnP	UPnP	Use this screen to enable UPnP on the EMG1302-R10A.
MAINTENANCE		
General	General	Use this screen to view and change administrative settings such as system and domain names.
Account	User Account	Use this screen to change the password of your EMG1302-R10A.
Time	Time Setting	Use this screen to change your EMG1302-R10A's time and date.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your EMG1302-R10A.
Backup/ Restore	Backup/ Restore	Use this screen to backup and restore the configuration or reset the factory defaults to your EMG1302-R10A.
Restart	System Restart	This screen allows you to reboot the EMG1302-R10A without turning the power off.

6

Tutorials

6.1 Overview

This chapter provides tutorials for setting up your EMG1302-R10A.

- Set Up a Wireless Network with WPS
- Configure Wireless Security without WPS
- Using Multiple SSIDs on the EMG1302-R10A

6.2 Set Up a Wireless Network with WPS

This section gives you an example of how to set up wireless network using WPS. This example uses the EMG1302-R10A as the AP and as the wireless client which connects to a notebook.

Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCI card).

There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See Section 6.2.1 on page 41.This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the EMG1302-R10A's interface. See Section 6.2.2 on page 42. This is the more secure method, since one device can authenticate the other.

6.2.1 Push Button Configuration (PBC)

1. Make sure that your EMG1302-R10A is turned on. Make sure the device is placed within range of your computer.
2. Make sure that you have installed the wireless client (this example uses the) driver and utility in your notebook.
3. In the wireless client utility, find the WPS settings. Enable WPS and press the WPS button (**Start** or **WPS** button).
4. Log into EMG1302-R10A's Web Configurator and press the **Push Button** in the **Configuration** > **Network** > **Wireless LAN** > **WPS Station** screen.

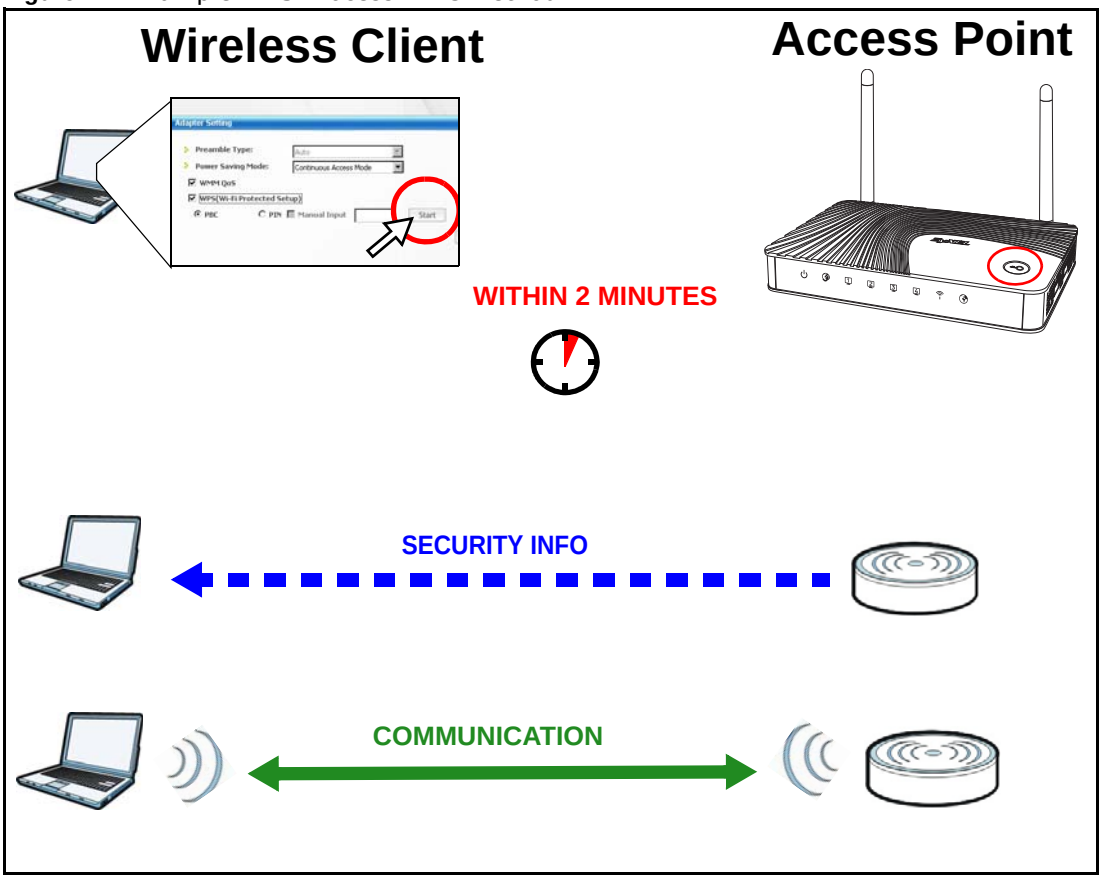
Note: Your EMG1302-R10A has a WPS button located on top panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

Note: It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

The EMG1302-R10A sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the EMG1302-R10A securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both EMG1302-R10A and wireless client (the in this example).

Figure 22 Example WPS Process: PBC Method



6.2.2 PIN Configuration

When you use the PIN configuration method, you need to use both EMG1302-R10A's configuration interface and the client's utilities.

1 Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.

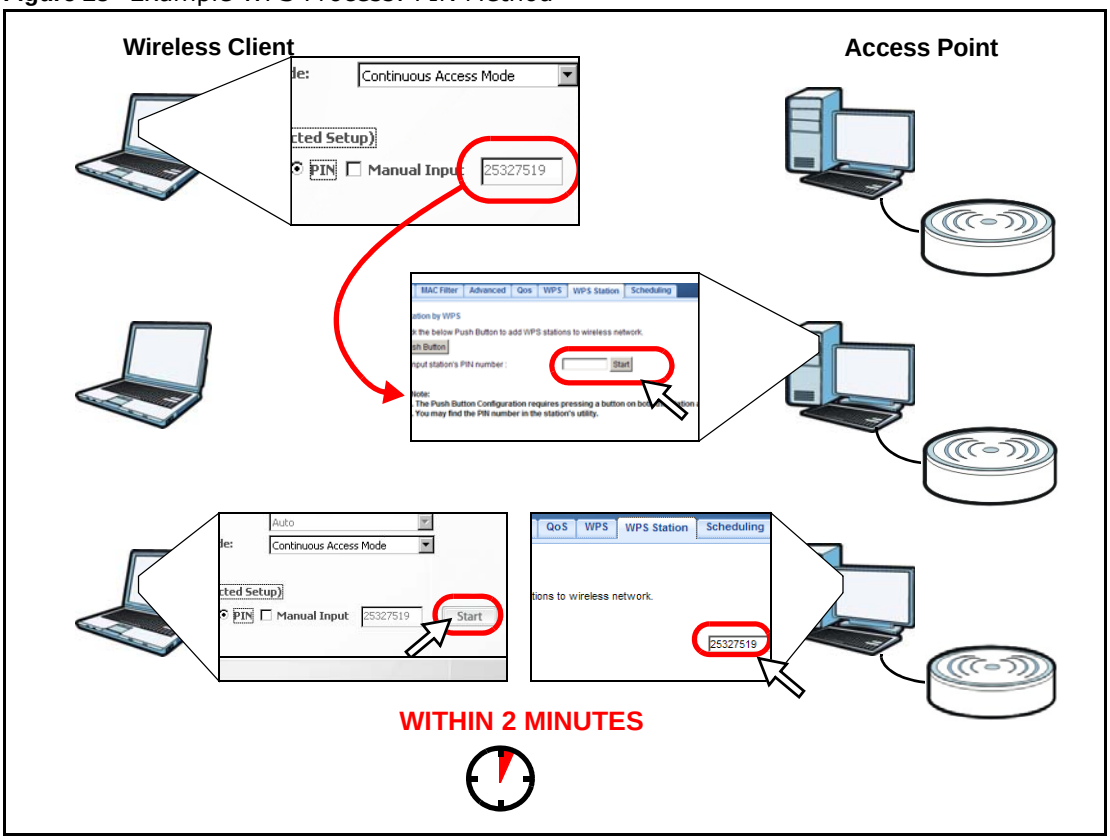
2 Enter the PIN number to the **PIN** field in the **Configuration** > **Network** > **Wireless LAN** > **WPS Station** screen on the EMG1302-R10A.

3 Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the EMG1302-R10A's **WPS Station** screen within two minutes.

The EMG1302-R10A authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the EMG1302-R10A securely.

The following figure shows you the example to set up wireless network and security on EMG1302-R10A and wireless client (ex. in this example) by using PIN method.

Figure 23 Example WPS Process: PIN Method



6.3 Configure Wireless Security without WPS

This example shows you how to configure wireless security settings with the following parameters on your EMG1302-R10A.

SSID	SSID_Example
Channel	6
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

Follow the steps below to configure the wireless settings on your EMG1302-R10A.

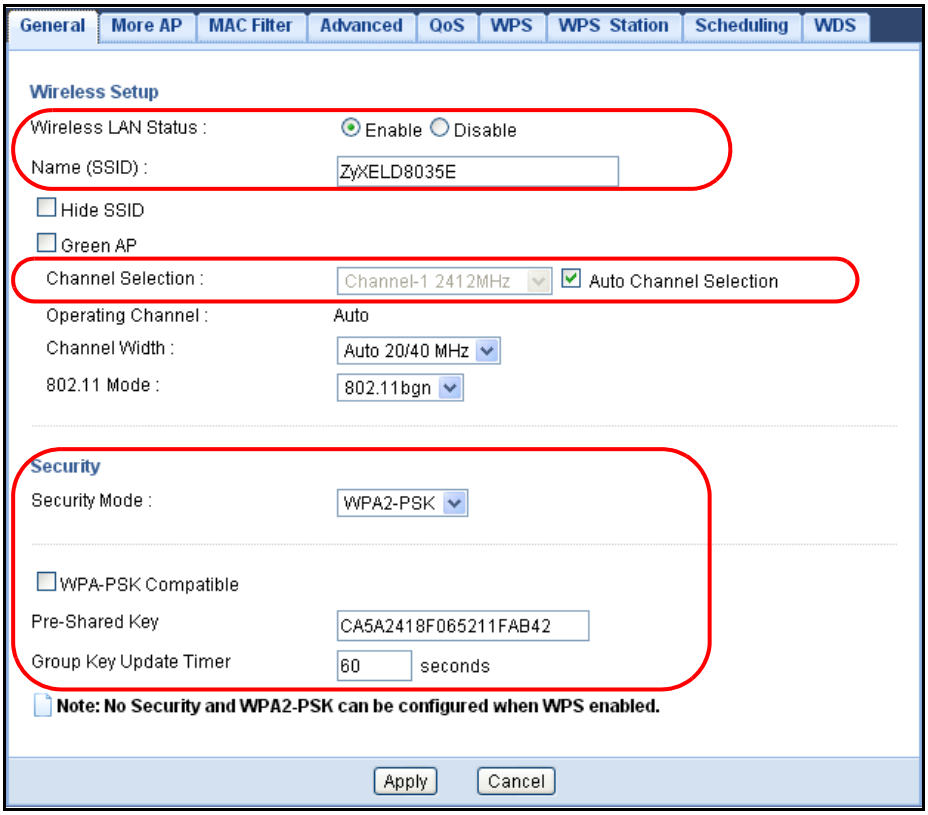
The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the Web Configurator through your LAN connection (see Section 2.3 on page 17).

1 Make sure the **WLAN** switch (at the back panel of the EMG1302-R10A) is set to **ON**.

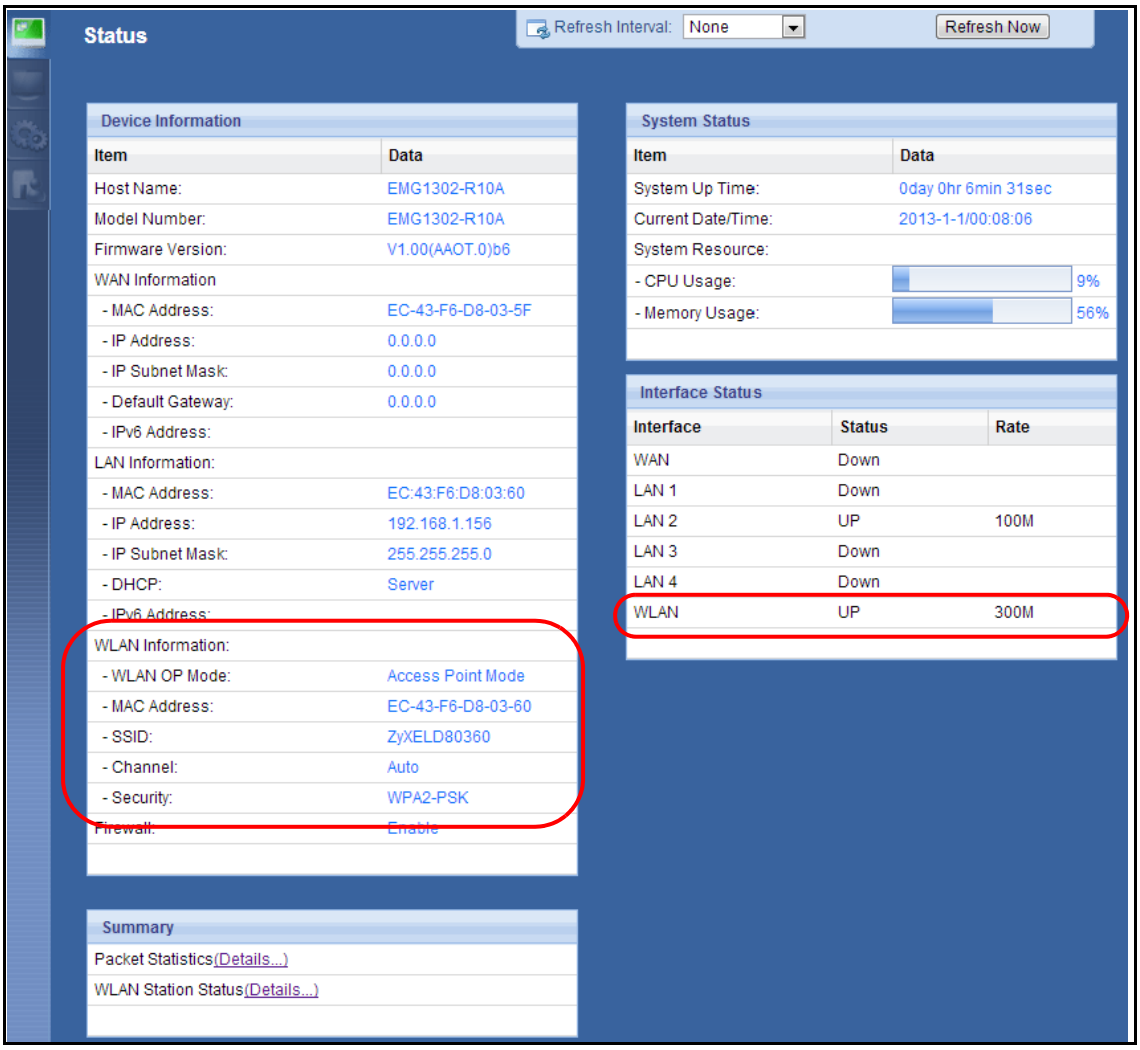
2 Open the **Configuration** > **Network** > **Wireless LAN** > **General** screen in the AP's Web Configurator.

3 Confirm that the status of wireless LAN is **ON**.

4 Enter **SSID_Example3** as the SSID and select **Channel-06** as the channel. Set security to **WPA2-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.l



5 Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.



6.3.1 Configure Your Notebook

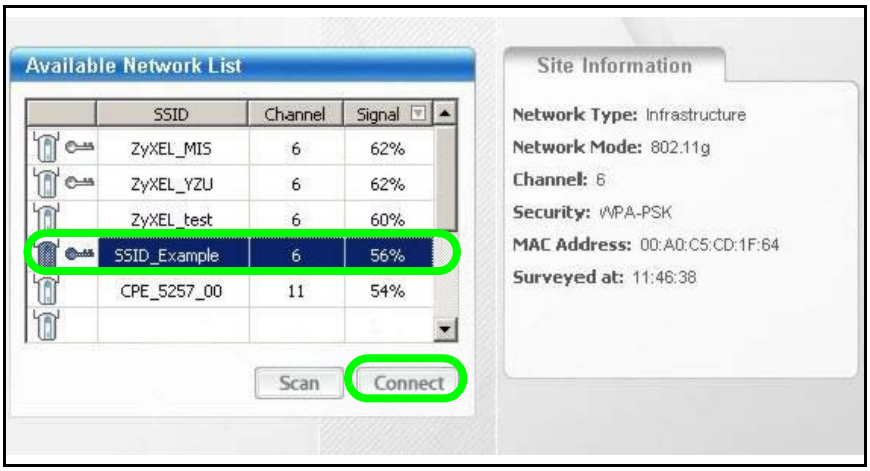
Note: We use the ZyXEL M-302 wireless adapter utility screens as an example for the wireless client. The screens may vary for different models.

1 The EMG1302-R10A supports IEEE 802.11b, IEEE 802.11g and IEEE 802.11n wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

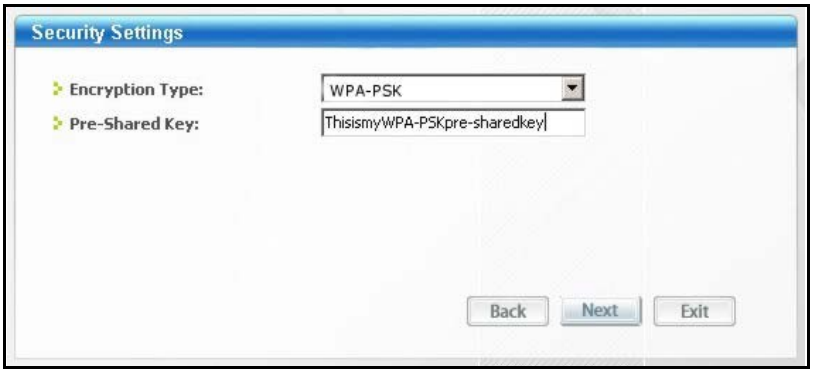
2 Wireless adapters come with software sometimes called a "utility" that you install on your computer. See your wireless adapter's User's Guide for information on how to do that.

3 After you've installed the utility, open it. If you cannot see your utility's icon on your screen, go to **Start > Programs** and click on your utility in the list of programs that appears. The utility displays a list of APs within range, as shown in the example screen below.

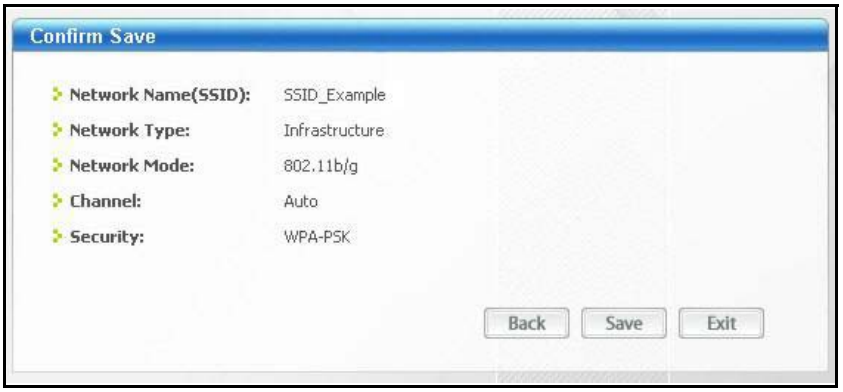
4 Select SSID_Example3 and click **Connect**.



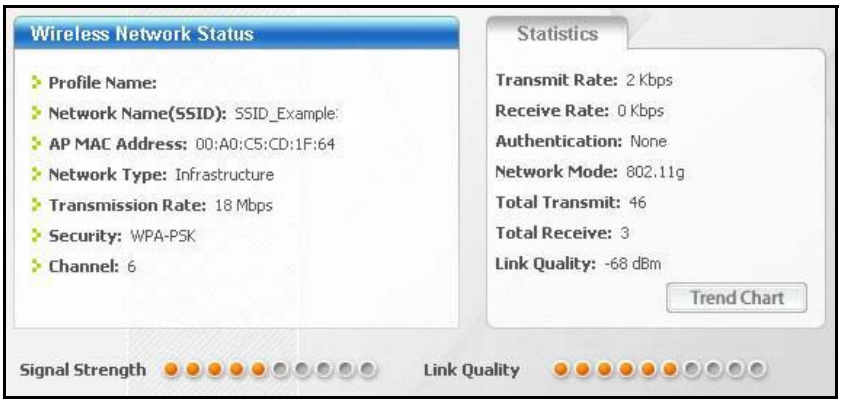
5 Select WPA-PSK and type the security key in the following screen. Click **Next**.



6 The **Confirm Save** window appears. Check your settings and click **Save** to continue.



7 Check the status of your wireless connection in the screen below. If your wireless connection is weak or you have no connection, see Chapter 22 Troubleshooting section of this User's Guide.



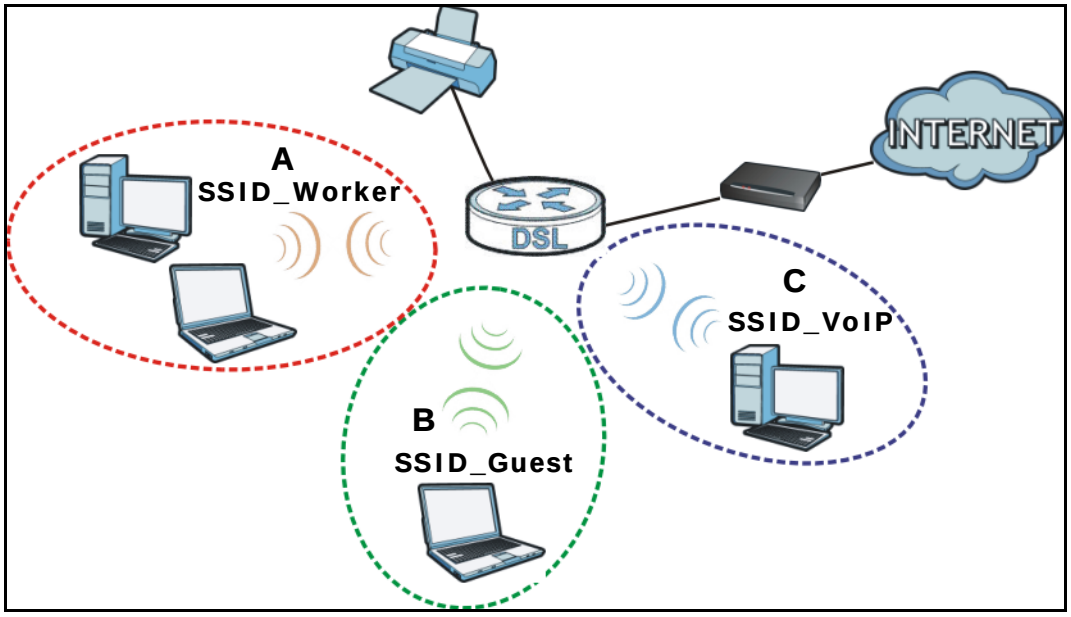
If your connection is successful, open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

6.4 Using Multiple SSIDs on the EMG1302-R10A

You can configure more than one SSID on a EMG1302-R10A when it is operating in access point or universal repeater mode. This allows you to configure multiple independent wireless networks on the EMG1302-R10A as if there were multiple APs (virtual APs). Each virtual AP has its own SSID, wireless security type and MAC filtering settings. That is, each SSID on the EMG1302-R10A represents a different access point/wireless network to wireless clients in the network.

Clients can associate only with the SSIDs for which they have the correct security settings. Clients using different SSIDs can access the Internet and the wired network behind the EMG1302-R10A (such as a printer). You can allow communication between wireless clients of different SSIDs in the **Configuration** > **Network** > **Wireless LAN** > **General** screen. See Section 8.4 on page 76 for more information.

For example, you may set up three wireless networks (**A**, **B** and **C**) in your office. **A** is for workers, **B** is for guests and **C** is specific to a VoIP device in the meeting room.



6.4.1 Configuring Security Settings of Multiple SSIDs

This example shows you how to configure the SSIDs with the following parameters on your EMG1302-R10A.

SSID	SECURITY TYPE	KEY	MAC FILTERING
SSID_Worker	WPA2-PSK WPA Compatible	DoNotStealMyWirelessNetwork	Disable
SSID_VoIP	WPA-PSK	VoIPOnly12345678	Allow 00:A0:C5:01:23:45
SSID_Guest	WPA-PSK	keyexample123	Disable

1 Connect your computer to the LAN port of the EMG1302-R10A using an Ethernet cable.

2 The default IP address of the EMG1302-R10A in router mode is "192.168.1.1". In this case, your computer must have an IP address in the range between "192.168.1.2" and "192.168.1.254".

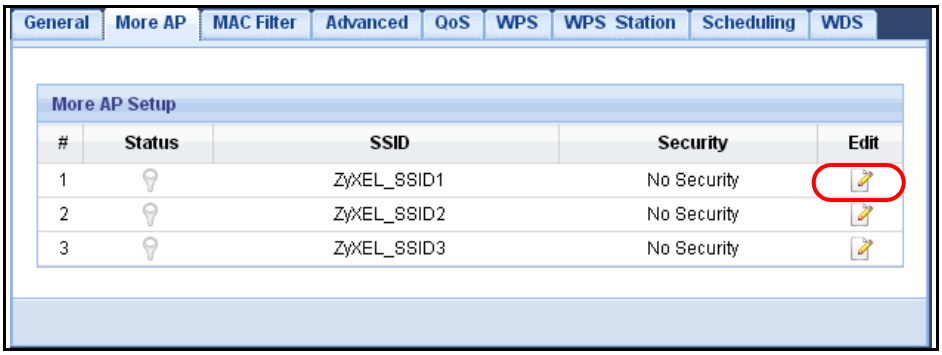
3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see Appendix C on page 251 for information on changing your computer's IP address.

4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://192.168.1.1" as the web address in your web browser.

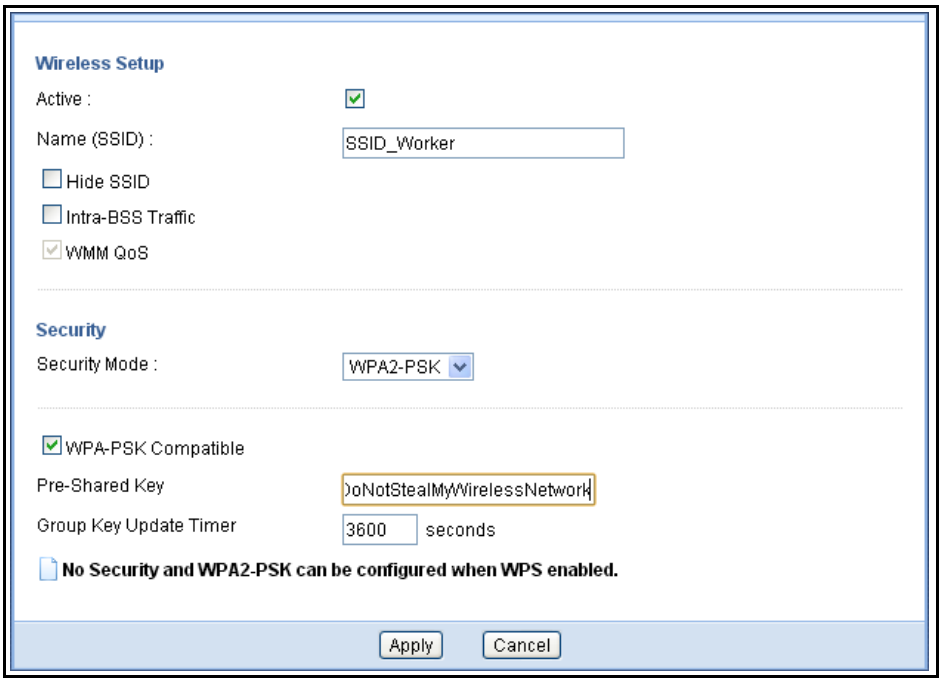
5 Enter "1234" (default) as the password and click **Login**.

6 Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.

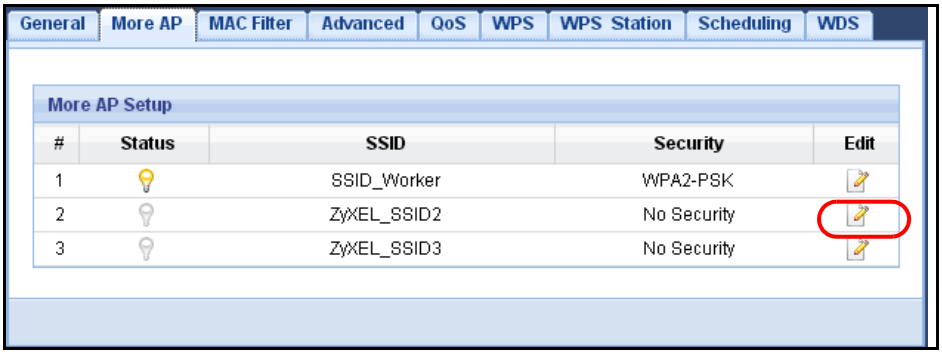
7 Go to **Configuration > Network > Wireless LAN > More AP**. Click the **Edit** icon of the first entry to configure wireless and security settings for **SSID_Worker**.



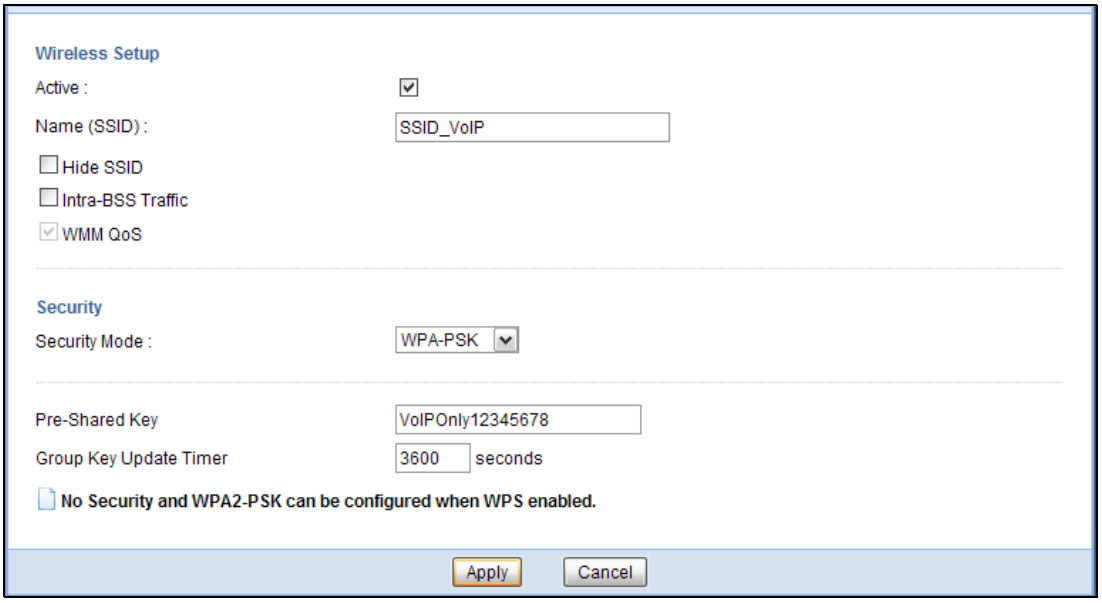
8 Configure the screen as follows. In this example, you enable **Intra-BSS Traffic** for **SSID_Worker** to allow wireless clients in the same wireless network to communicate with each other. Click **Apply**.



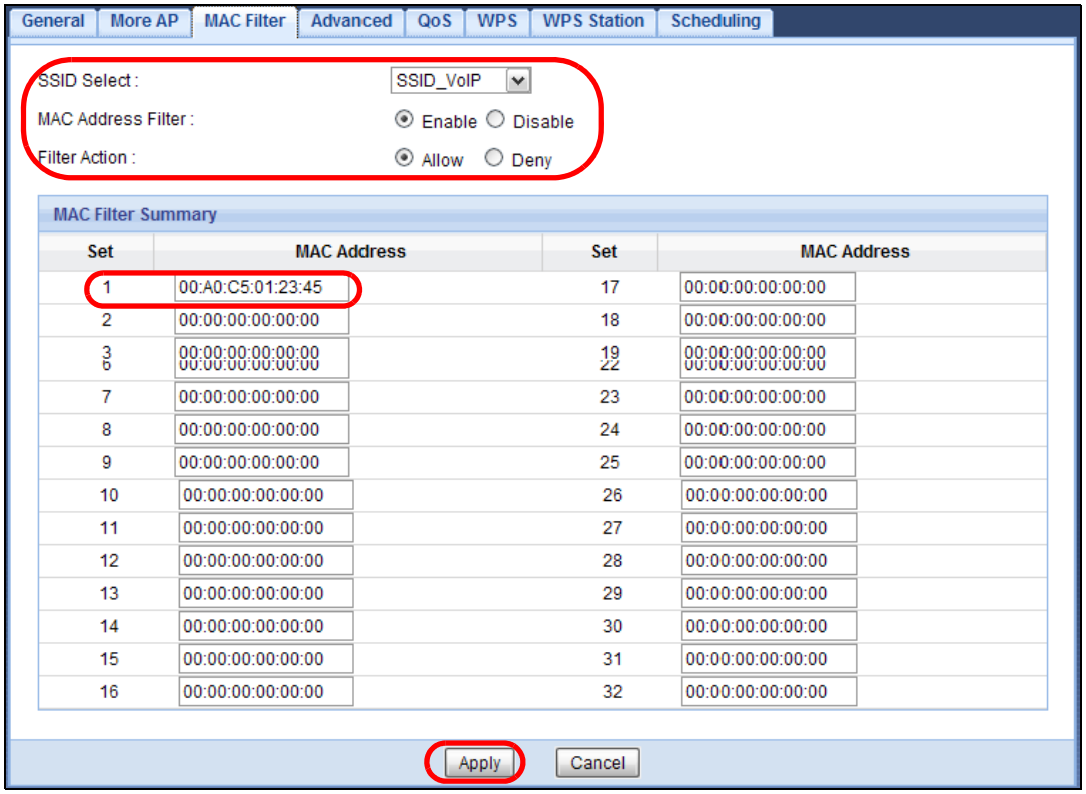
9 Click the **Edit** icon of the second entry to configure wireless and security settings for **SSID_VoIP**.



10 Configure the screen as follows. You do not enable **Intra-BSS Traffic** for **SSID_VoIP**. Click **Apply**.



11 Click the **MAC Filter** tab to configure MAC filtering for the **SSID_VoIP** wireless network. Select **SSID_VoIP** from the **SSID Select** drop-down list, enable MAC address filtering and set the **Filter Action** to **Allow**. Enter the VoIP device's MAC address in the **Mac Address** field and click **Apply** to allow only the VoIP device to associate with the EMG1302-R10A using this SSID.



PART II
Technical Reference

7

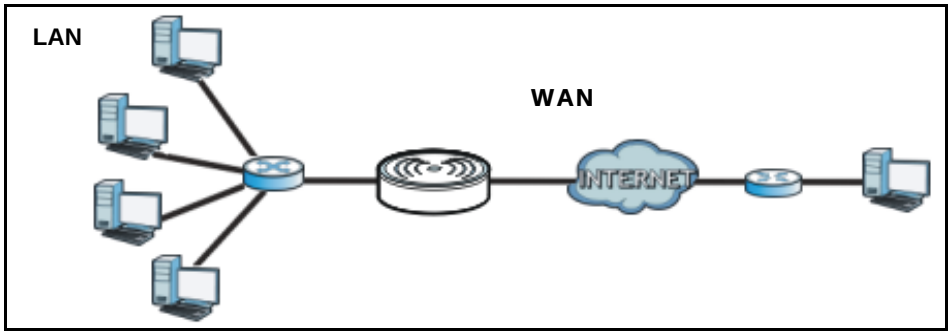
WAN

7.1 Overview

This chapter discusses the EMG1302-R10A's **WAN** screens. Use these screens to configure your EMG1302-R10A for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

Figure 24 LAN and WAN



7.2 What You Can Do

- Use the **Management WAN** screen to enter your ISP information and set how the computer acquires its IP, DNS and WAN MAC addresses (Section 7.4 on page 57).
- Use the **Advanced** screen to enable multicasting and auto-IP-change (Section 7.5 on page 70).

7.3 What You Need To Know

The information in this section can help you configure the screens for your WAN connection, as well as enable/disable some advanced features of your EMG1302-R10A.

7.3.1 Configuring Your Internet Connection

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet) or PPTP (Point-to-Point Tunneling Protocol), they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the EMG1302-R10A, which makes it accessible from an outside network. It is used by the EMG1302-R10A to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the EMG1302-R10A tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The EMG1302-R10A can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
2. If your ISP dynamically assigns the DNS server IP addresses (along with the EMG1302-R10A's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

WAN MAC Address

The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Clone the computer's MAC address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to configuration file. It is recommended that you clone the MAC address prior to hooking up the WAN Port.

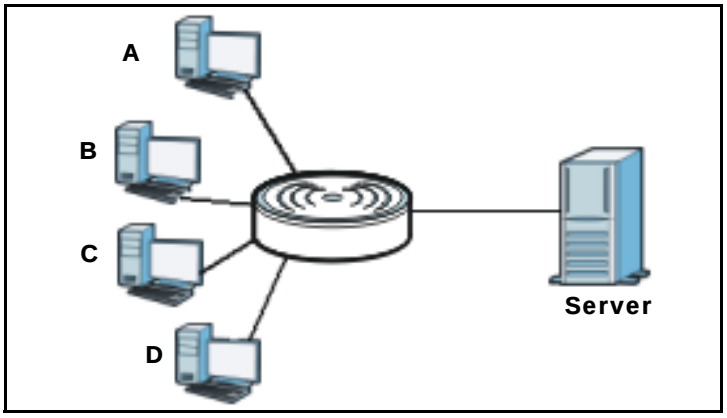
Maximum Transmission Unit

A maximum transmission unit (MTU) is the largest size packet or frame, specified in octets (eight-bit bytes) that can be sent in a packet- or frame-based network. The Transmission Control Protocol (TCP) uses the MTU to determine the maximum size of each packet in any transmission. Too large an MTU size may mean retransmissions if the packet encounters a router that can't handle that large a packet. Too small an MTU size means relatively more header overhead and more acknowledgements that have to be sent and handled.

7.3.2 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

Figure 25 Multicast Example



In the multicast example above, systems A and D comprise one multicast group. In multicasting, the server only needs to send one data stream and this is delivered to systems A and D.

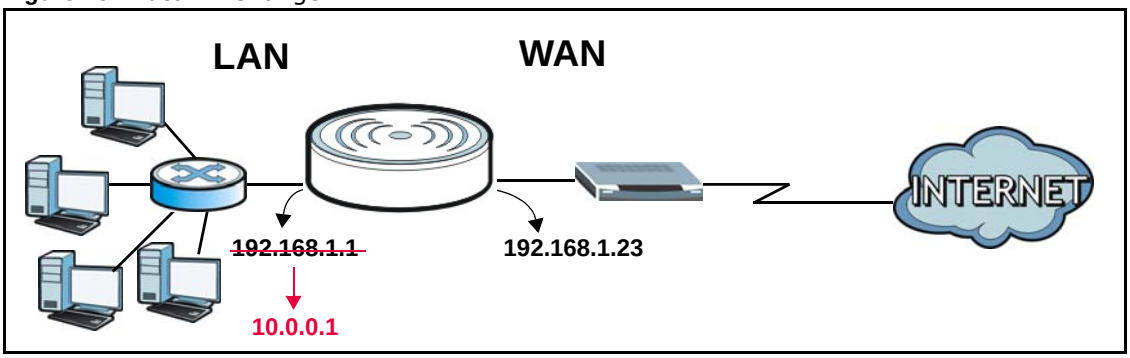
IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. The EMG1302-R10A supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**).

At start up, the EMG1302-R10A queries all directly connected networks to gather group membership. After that, the EMG1302-R10A periodically updates this information. IP multicasting can be enabled/disabled on the EMG1302-R10A LAN and/or WAN interfaces in the Web Configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

Auto-IP-Change

When the EMG1302-R10A gets a WAN IP address which is in the same subnet as the LAN IP address 192.168.1.1, Auto-IP-Change allows the EMG1302-R10A to change its LAN IP address to 10.0.0.1 automatically. If the EMG1302-R10A's original LAN IP address is 10.0.0.1 and the WAN IP address is in the same subnet, such as 10.0.0.3, the EMG1302-R10A switches to use 192.168.1.1 as its LAN IP address.

Figure 26 Auto-IP-Change



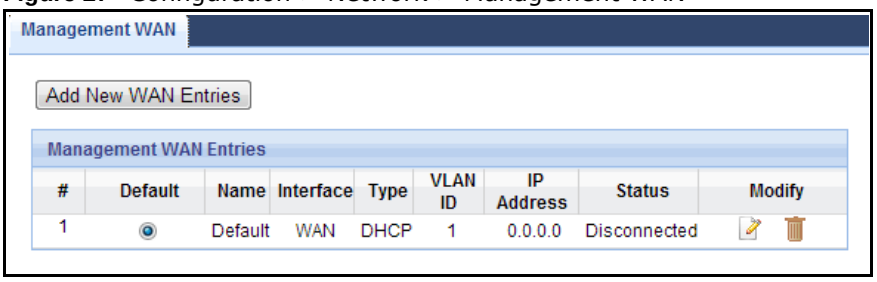
Auto-IP-Change only works under the following conditions:

- The EMG1302-R10A must be in **Router Mode** (see Chapter 21 on page 158 for more information) for Auto-IP-Change to become active.
- The EMG1302-R10A is set to receive a dynamic WAN IP address using the Ethernet or PPPoE connection type.

7.4 Management WAN

Use this screen to view, change, or add your EMG1302-R10A's Internet access settings. Click **Configuration** > **Network** > **WAN**. The following screen opens.

Figure 27 Configuration > Network > Management WAN


Management WAN
Add New WAN Entries
Management WAN Entries
Default Name Interface Type VLAN ID IP Address Status Modify
1 Default WAN DHCP 1 0.0.0.0 Disconnected

The following table describes the labels in this screen.

Table 11 Configuration > Network > Management WAN

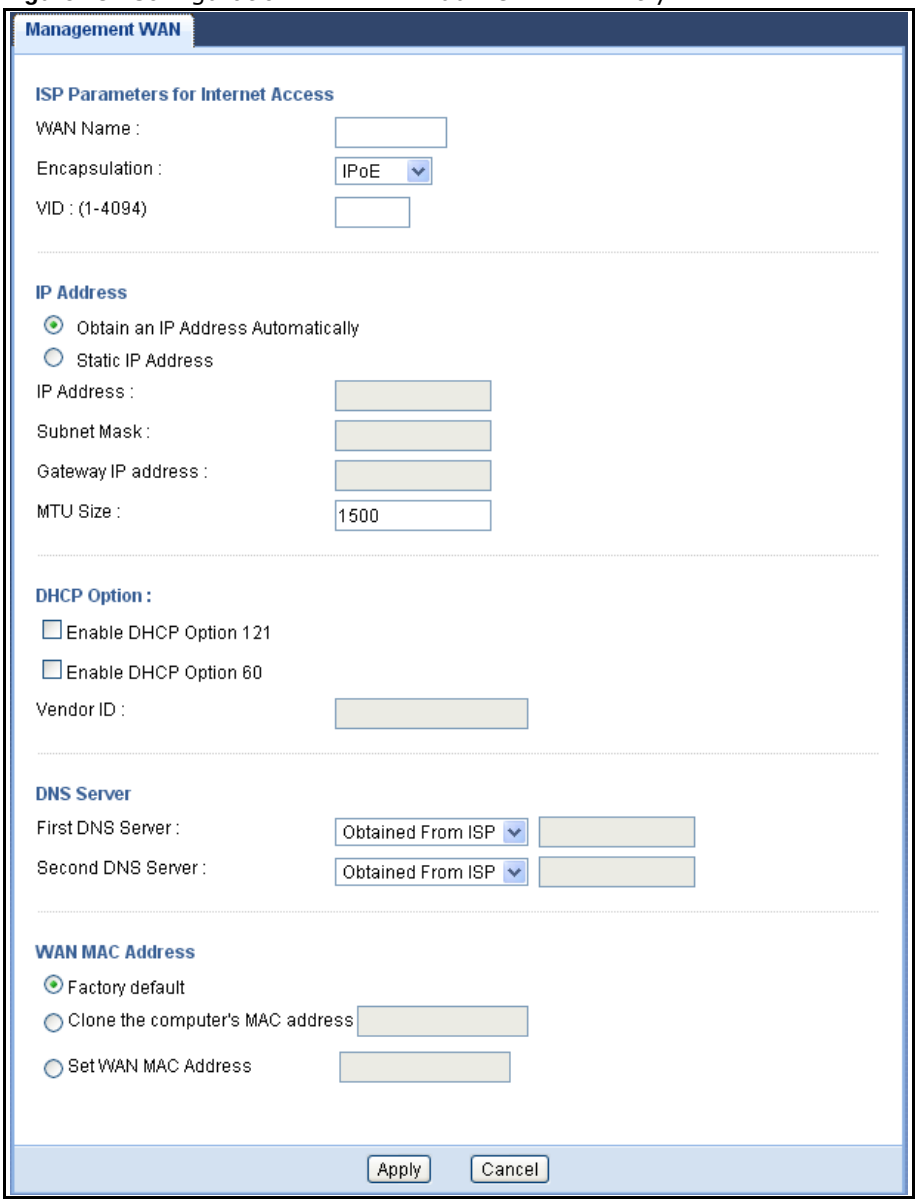
LABEL	DESCRIPTION
Add New WAN Entry	Click this to create a new WAN interface entry.
#	This is the index number of the connection.
Default	Select the WAN interface that you want to configure as default.
Name	This is the service name of the connection.
Interface	This is the interface of the connection.
Type	This shows the type of interface used by this connection.
VLAN ID	This indicates the VLAN ID number assigned to traffic sent through this connection.
IP Address	This is the WAN IP address used by this connection.
Status	This shows the status of the connection.
Modify	Click the **Edit** icon to configure the connection. Click the **Delete** icon to delete this connection from the EMG1302-R10A. A window displays asking you to confirm that you want to delete the connection.

7.4.1 Add/Edit Internet Connection

Click the **Add New WAN Entry** in the **Configuration** > **WAN** screen or the **Edit** icon next to the connection you want to configure. Use this screen to configure a WAN connection. The screen varies depending on the encapsulation you select.

This screen displays when you select **Add New WAN Entry** encapsulation.

Figure 28 Configuration > WAN > Add New WAN Entry



The following table describes the labels in this screen.

Table 12 Configuration > WAN > Add New WAN Entry

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
WAN Name	Enter the name designation for this setting. Note: Only the following parameters are available in Bridge mode: WAN name, encapsulation and VID.
Encapsulation	Select the encapsulation type: **PPPoE**, **PPTP**, **IPoE**, or **Bridge**.
VID (1~4094)	Enter a VLAN identifier between 1 to 4094 (the 802.1Q tag specifies only a priority and is referred to as a priority tag). In bridge mode, VID 1 (the default VLAN ID) is reserved for a management VLAN.
IP Address	Select **Obtain an IP Address Automatically** to have your ISP assign the parameters. Select **Static IP Address** to enter a pre-defined IP Address, Subnet Mask, and Gateway IP address.
MTU Size	Enter the Maximum Transmission Unit (MTU) or the largest packet size per frame that your EMG1302-R10A can receive and process.
DHCP Option	
Enable DHCP Option 121	Select Enable DHCP Option 121 to enable the classless route option 121.
Enable DHCP Option 60	Select Enable DHCP Option 60 to enable and enter the device's Vendor Class Identifier (VCI).
DNS Server	
First DNS Server Second DNS Server	If you select **Get automatically from ISP (Default)** in the **WAN IP Address Assignment** section, this field will automatically be set to **From ISP**. The field to the right displays the (read-only) DNS server IP address that the ISP assigns. If you select **Use Fixed IP Address** in the **WAN IP Address Assignment** section, this field will automatically be set to **User-Defined**. Enter the DNS server's IP address in the field to the right.
WAN MAC Address	
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the EMG1302-R10A's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address	Select **Clone the computer's MAC address** and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

7.4.1.1 PPPoE Encapsulation

The EMG1302-R10A supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPP over Ethernet** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius).

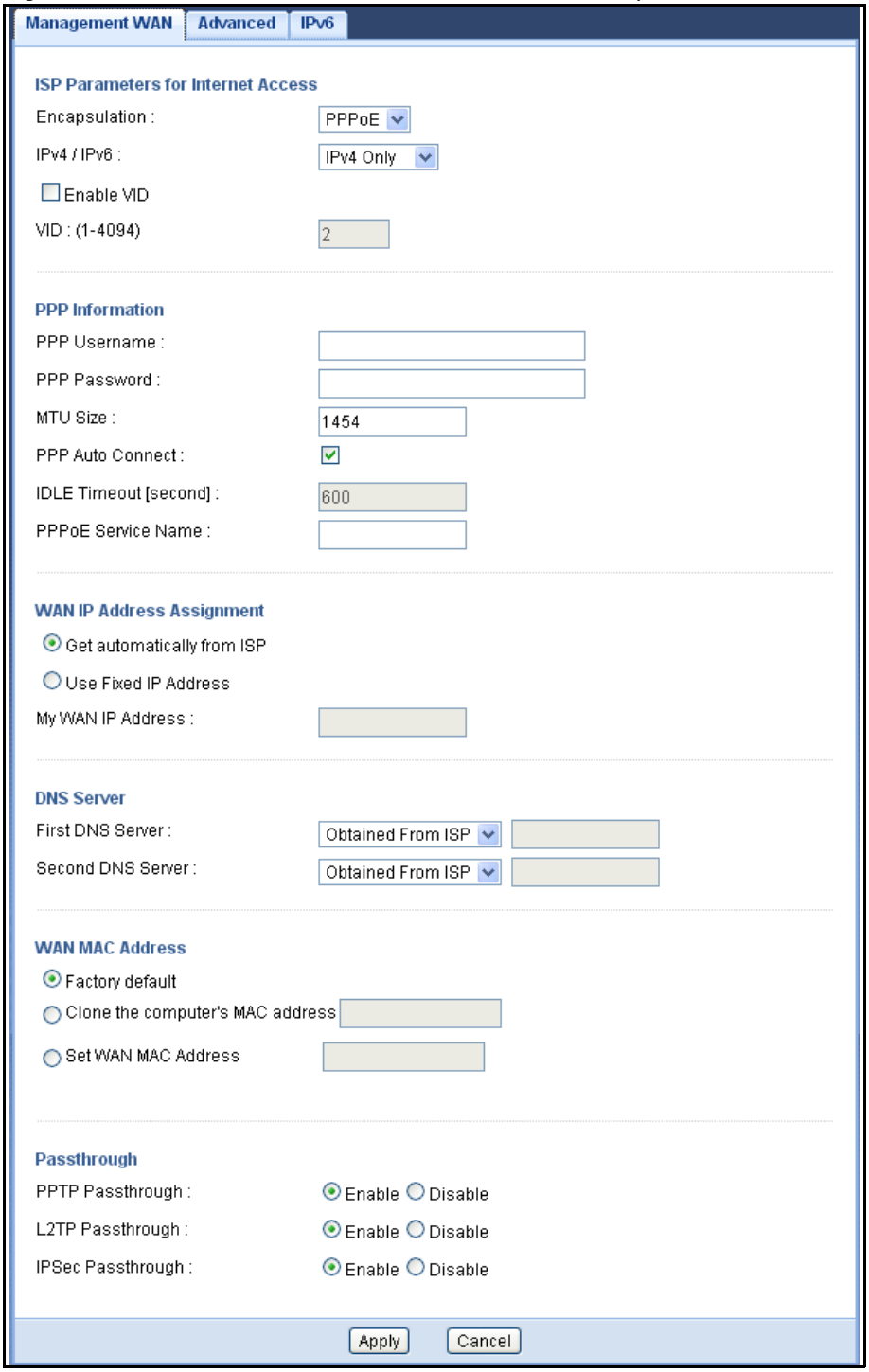
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the EMG1302-R10A (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the EMG1302-R10A does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

This screen displays when you select **PPP over Ethernet** encapsulation.

Figure 29 Internet Connection: PPP over Ethernet Encapsulation



The following table describes the labels in this screen.

Table 13 Internet Connection: PPP over Ethernet Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select **PPP over Ethernet** if you connect to your Internet via dial-up.
IPv4 / IPv6	Click the drop-down menu to select either an **IPv4 Only** or **dual stack interface**.
Enable VID	
VID (1~4094)	Enter a VLAN identifier between 1 to 4094 (the 802.1Q tag specifies only a priority and is referred to as a priority tag). In bridge mode, VID 1 (the default VLAN ID) is reserved for a management VLAN.
PPP Information	
PPP Username	Enter the user name to use for logging in to the PPP service.
PPP Password	Enter the password to associate with the PPP user name (previous field).
MTU Size	Enter the Maximum Transmission Units (MTU) in bytes (default: 1454, range: 68 to 1492).
PPP Auto Connect	Click to enable the PPP auto connect function when the service is disconnected.
IDLE Timeout (second)	Enter a variable (seconds) to designate the timeout period during an idle session.
PPPoE Service Name	Enter the name to designate the service.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
DNS Server	
First DNS Server Second DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the EMG1302-R10A's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the EMG1302-R10A's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address	Select **Clone the computer's MAC address** and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.

Table 13 Internet Connection: PPP over Ethernet Encapsulation (continued)

LABEL	DESCRIPTION
Passthrough	
PPTP Passthrough	
L2TP Passthrough	
IPSec Passthrough	
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

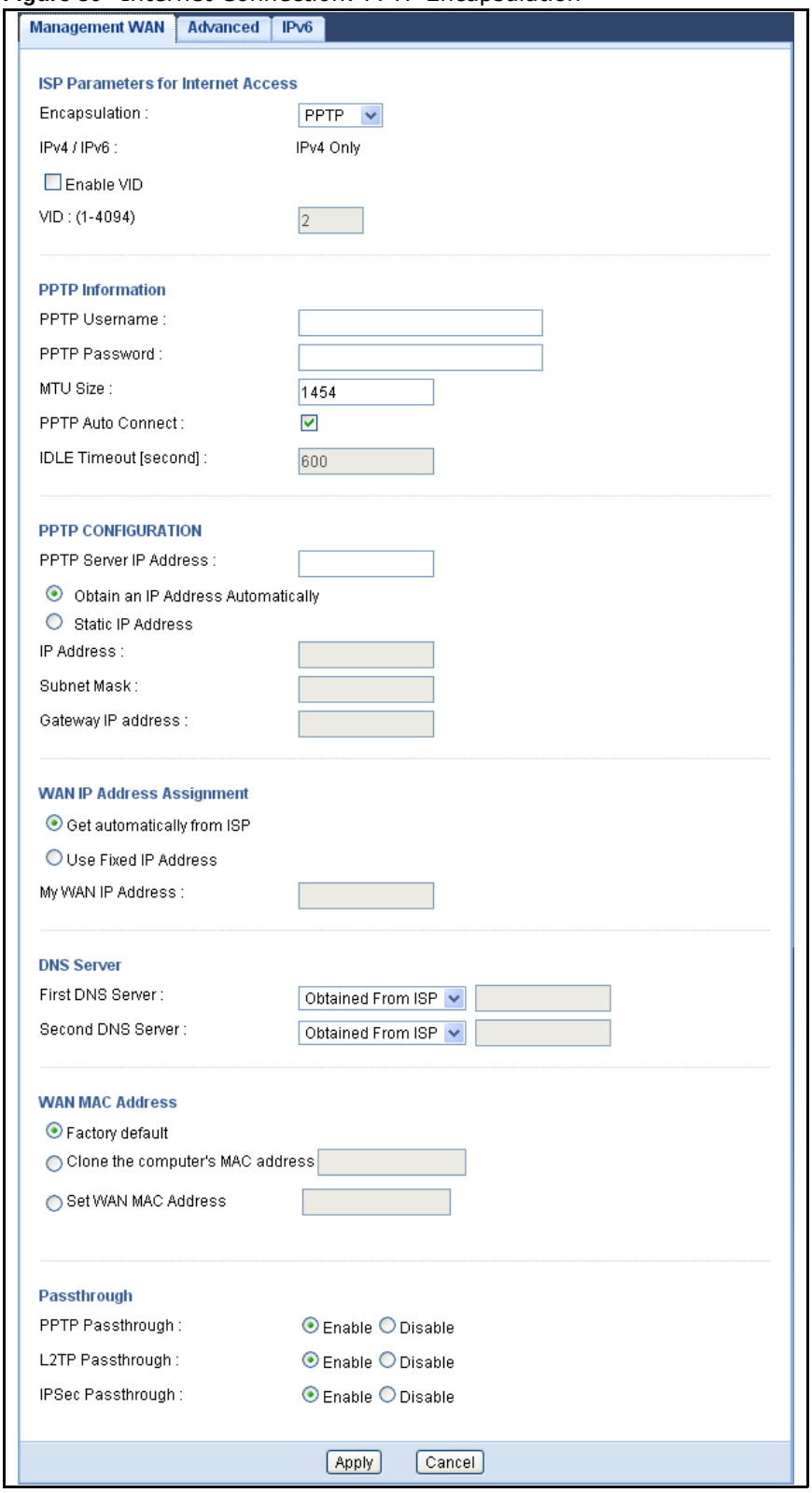
7.4.1.2 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

This screen displays when you select **PPTP** encapsulation.

Figure 30 Internet Connection: PPTP Encapsulation



The following table describes the labels in this screen.

Table 14 Internet Connection:PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select **PPTP** to create a Virtual Private Network (VPN) using TCP/IP-based network.
Enable VID	
VID (1~4094)	Enter a VLAN identifier between 1 to 4094 (the 802.1Q tag specifies only a priority and is referred to as a priority tag). In bridge mode, VID 1 (the default VLAN ID) is reserved for a management VLAN.
PPTP Information	
PPTP Username	Type the username given to you by your ISP.
PPTP Password	Type the password associated with the user name above.
MTU Size	Enter the Maximum Transmission Unit (MTU) or the largest packet size per frame that your EMG1302-R10A can receive and process.
PPTP Auto Connect	Select this check box to enable PPTP Auto Connect.
IDLE Timeout (second)	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server.
PPTP Configuration	
PPTP Server IP Address	Type the IP address of the PPTP server.
Obtain an IP Address Automatically	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Static IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Static IP Address**.
Subnet Mask	Your EMG1302-R10A will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the EMG1302-R10A.
Gateway IP address	Enter a **Gateway IP Address** (if your ISP gave you one) in this field.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
DNS Server	
First DNS Server Second DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the EMG1302-R10A's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.

Table 14 Internet Connection:PPTP Encapsulation (continued)

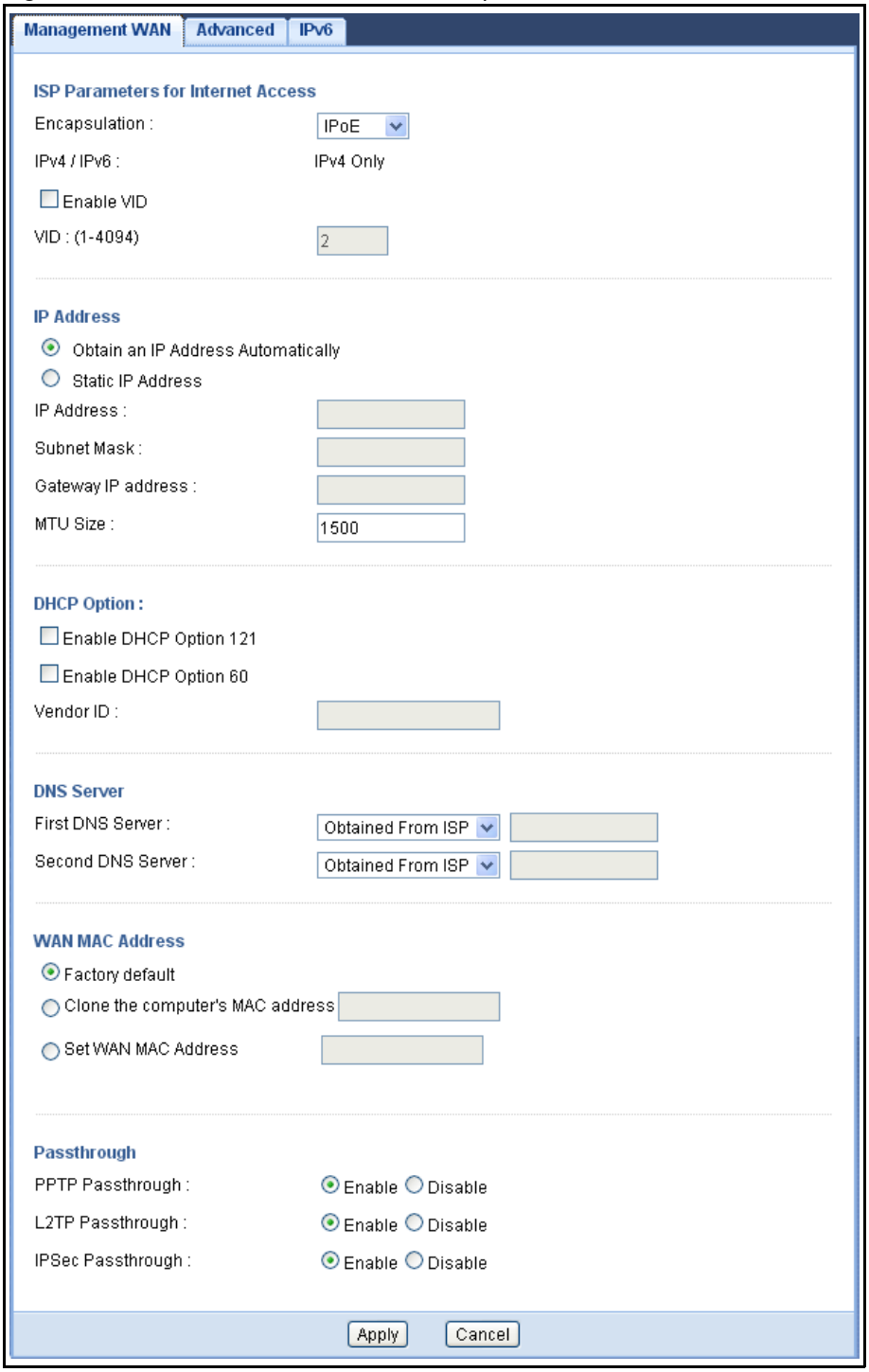
LABEL	DESCRIPTION
WAN MAC Address	
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address	Select **Clone the computer's MAC address** and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Passthrough	
PPTP Passthrough	
L2TP Passthrough	
IPSec Passthrough	
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

7.4.1.3 IPoE Encapsulation

IP over Ethernet is an alternative to PPP encapsulation. In IPoE DHCP extensions and other protocols, like for example Extensible Authentication Protocol, are combined with DHCP to provide capabilities similar to PPPoE. You can configure the WAN connection with IPoE to use NAT, firewall or IGMP proxy in EMG1302-R10A.

This screen displays when you select **IPoE** encapsulation.

Figure 31 Internet Connection: IPoE Encapsulation



The following table describes the labels in this screen.

Table 15 Internet Connection: IP over Ethernet Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the **IPoE** option when the WAN port is used as a regular Ethernet.
IPv4 / IPv6	Click the drop down menu to select the available options: **IPv4 only**, **dual stack**, or **IPv6**.
Enable VID	
VID (1~4094)	Enter a VLAN identifier between 1 to 4094 (the 802.1Q tag specifies only a priority and is referred to as a priority tag). In bridge mode, VID 1 (the default VLAN ID) is reserved for a management VLAN.
IP Address	
Obtain an IP Address Automatically	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Static IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Static IP Address**.
Subnet Mask	Your EMG1302-R10A will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the EMG1302-R10A.
Gateway IP address	Enter a **Gateway IP Address** (if your ISP gave you one) in this field.
MTU Size	Enter the Maximum Transmission Unit (MTU) or the largest packet size per frame that your EMG1302-R10A can receive and process.
DHCP Option	
Enable DHCP Option 121	Select Enable DHCP Option 121 to enable the classless route option 121.
Enable DHCP Option 60	Select Enable DHCP Option 60 to enable and enter the device's Vendor Class Identifier (VCI).
DNS Server	
First DNS Server Second DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the EMG1302-R10A's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the EMG1302-R10A's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address	Select **Clone the computer's MAC address** and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.

Table 15 Internet Connection: IP over Ethernet Encapsulation (continued)

LABEL	DESCRIPTION
Passthrough	
PPTP Passthrough	
L2TP Passthrough	
IPSec Passthrough	
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

7.4.2 Bridge Encapsulation

This screen displays when you select **Bridge** encapsulation.

Figure 32 Internet Connection: Bridge Encapsulation

The following table describes the labels in this screen.

Table 16 Internet Connection: Bridge Encapsulation

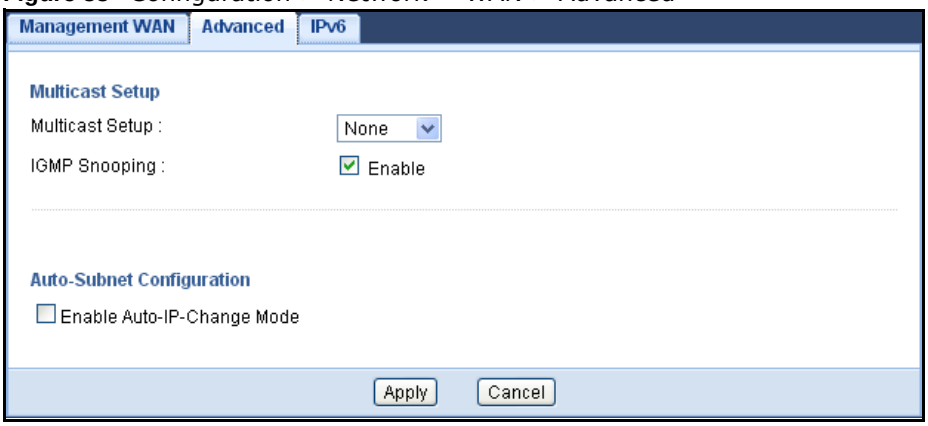
LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use routing functions, such as DHCP server. The function is currently available for the IPv4 protocol.
Enable VID	
VID (1~4094)	Enter a VLAN identifier between 1 to 4094 (the 802.1Q tag specifies only a priority and is referred to as a priority tag). In bridge mode, VID 1 (the default VLAN ID) is reserved for a management VLAN.
Ignore WAN Vlan ID when tag frame reveive from LAN site	
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

7.5 Advanced WAN Screen

Use this screen to enable **Multicast** and enable **Auto-IP-Change** mode.

To change your EMG1302-R10A's advanced WAN settings, click **Configuration** > **Network** > **WAN** > **Advanced**. The screen appears as shown.

Figure 33 Configuration > Network **>** WAN > Advanced



The following table describes the labels in this screen.

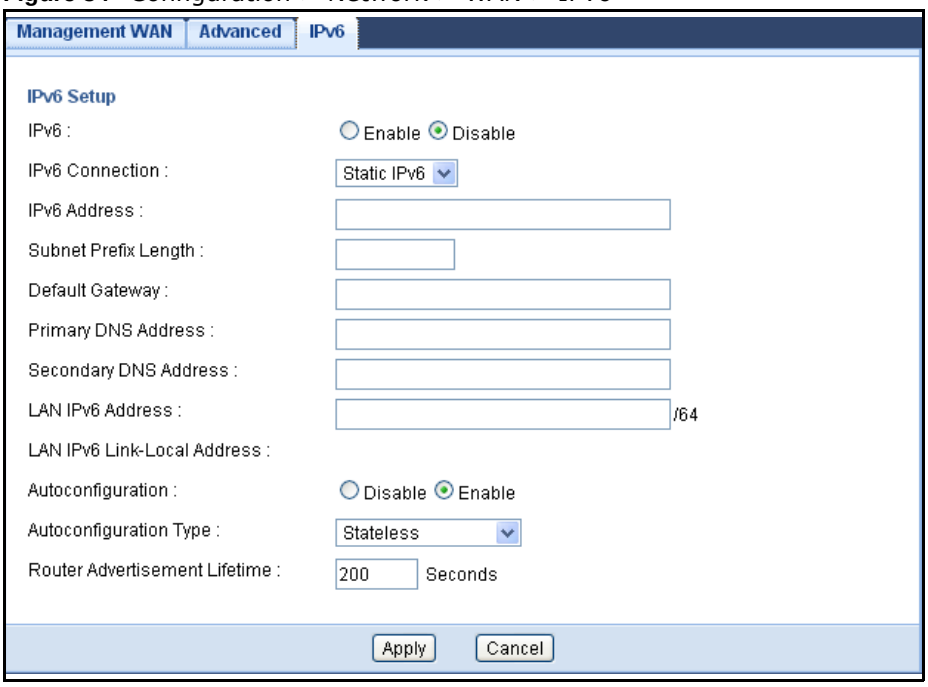
Table 17 Configuration > Network **>** WAN > Advanced

LABEL	DESCRIPTION
Multicast Setup	
Multicast Setup	Select **IGMPv1 / v2 / v3** to enable multicasting. This applies to traffic routed from the WAN to the LAN. Select **None** to disable this feature. This may cause incoming traffic to be dropped or sent to all connected network devices.
IGMP Snooping	The IGMP Snooping allows for listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows the ZyXEL device to listen in on the IGMP conversation between hosts and routers. This allows the ZyXEL device to map links to determine which map links require IP multicast streams. Select this check box to use the IGMP Snooping function.
Auto-Subnet Configuration	
Enable Auto-IP-Change Mode	Select this option to have the EMG1302-R10A switch to bridge mode automatically when the EMG1302-R10A gets a WAN IP address in the range of 192.168.x.y (where x and y are from zero to nine) no matter what the LAN IP address is.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

7.6 IPv6 Screen

Use this section to enable and configure IPv6 addresses. By using IPv6, you are able to receive services such as: quality of service (QoS), end-to-end security, and globally unique addresses.

Figure 34 Configuration > Network > WAN > IPv6



The following table describes the labels in this screen.

Table 18 Configuration > Network > WAN > IPv6

LABEL	DESCRIPTION
IPv6 Setup	
IPv6	Select a field to Enable or Disable the IPv6 standard.
IPv6 Connection	Select the IPv6 connection type: Static IPv6, DHCPv6, PPoE, or 6rd.
IPv6	
IPv6 Address	Enter the IPv6 address specified in heaxadecimal using 16-bit values between colons.
Subnet Prefix Length	Enter the subnet prefix variable, a decimal value to define how many of the high-order contiguous bits of the address are the prefix.
Default Gateway	Enter the specified gateway to set as default for the IPv6 connection type.
DHCPv6	
DNC Setting	• Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es)**.** • If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Primary DNS server** and **Secondary DNS server** fields.
PPPoE	

Table 18 Configuration > Network > WAN > IPv6 (continued)

LABEL	DESCRIPTION
Address Mode	Click **Dynamic IP** if your ISP assigs an IP address. If you have a fixed IP address assigned to you, click **Static IP**, and type the I**P Address**, **Username** and **Password** in the following fields.
Username	Enter the username as it is assigned for this account.
Password	Enter the designated password for the username in the previous field..
Service Name	Enter a name to assign this service.
Reconnect Mode	Select **Auto Reconnect (always-on)** to have the Reconnect Mode continuously connected. Select **Connect-on-Demand** to have the Reconnect Mode only active when WAN service is active. Select **Manually** to only allow WAN reconnection if manually initiated by a user.
Maximum Idle Time	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
Remote IPv4 Address	Enter the designated IPv4 address to allow tunneling across ISP network.
Remote PREFIX	Enter the IPv6 prefix for the PPPoE tunnel.
6RD	
Remote IPv4 Address	Enter the designated IPv4 address to allow tunneling across an ISP network.
Remote PREFIX	Enter the IPv6 prefix for the 6RD tunnel. This is only available if 6RD Static-type is designated.
Primary DNS Address	Enter the primary DNS server address assigned by the ISP.
Secondary DNS Address	Enter the secondary DNS server address assigned by the ISP.
LAN IPv6 Address	Enter the static IPv6 address assigned to this device.
LAN IPv6 Link-Local Address	The system assigns a local address designed for use on a single link.
Autoconfiguration	Enable/Disable the auto IP address configuration setting.
Autoconfiguration Type	If autoconfiguration is enabled, the following types are available: IP address, stateful, and stateless.
Router Advertisement Lifetime	The device refreshes the preferred and valid time with each advertisement message. The device is configured with a valid lifetime value for each network prefix, broadcasted in the advertisement message.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

8

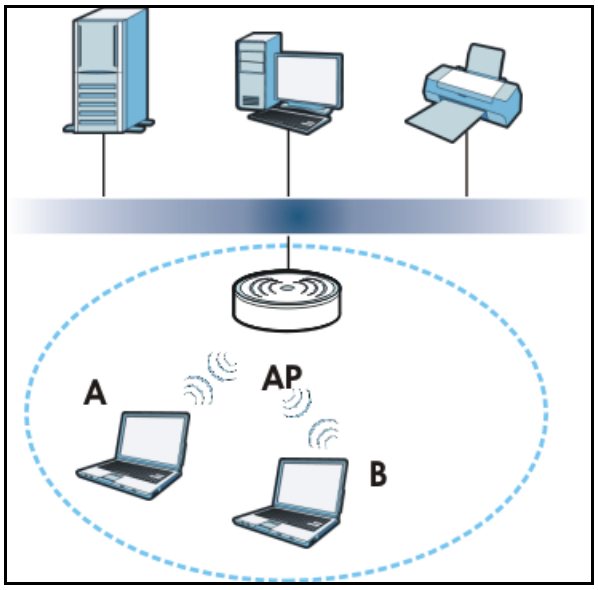
Wireless LAN

8.1 Overview

This chapter discusses how to configure the wireless network settings in your EMG1302-R10A. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 35 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices A and B are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your EMG1302-R10A is the AP.

8.2 What You Can Do

- Use the **General** screen to enter the SSID, select the channel, and configure wireless security (Section 8.4 on page 76).
- Use the **More AP** screen to enable and configure multiple wireless networks (Section 8.6 on page 81)
- Use the **MAC Filter** screen to allow or deny wireless stations based on their MAC addresses from connecting to the EMG1302-R10A (Section 8.7 on page 83).
- Use the **Advanced** screen to allow intra-BSS network and set the RTS/CTS Threshold (Section 8.8 on page 84).

- Use the **QoS** screen to ensure Quality of Service (QoS) in your wireless network (Section 8.9 on page 85).
- Use the **WPS** screen to quickly set up a wireless network with strong security, without having to configure security settings manually (Section 8.10 on page 86).
- Use the **WPS Station** screen to add a wireless station using WPS (Section 8.11 on page 87).
- Use the **Scheduling** screen to set the times your wireless LAN is turned on and off (Section 8.12 on page 88).
- Use the **WDS** screen to set up Wireless Distribution System (WDS) (Section 8.13 on page 89).

8.3 What You Should Know

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every wireless client in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or

1.Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

2.Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized wireless client. Then, they can use that MAC address to use the wireless network.

User Authentication

You can make every user log in to the wireless network before they can use it. This is called user authentication.

For wireless networks, there are two typical places to store the user names and passwords for each user.

- In the AP: this feature is called a local user database or a local database.
- In a RADIUS server: this is a server used in businesses more than in homes.

If your AP does not provide a local user database and if you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

Local user databases also have an additional limitation that is explained in the next section.

Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of user authentication. (See page 75 for information about this.)

Table 19 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
↕	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. For example, suppose the AP does not have a local user database, and you do not have a RADIUS server. Therefore, there is no user authentication. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. IEEE and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

Note: It is not possible to use **WPA-PSK**, **WPA** or stronger encryption with a local user database. In this case, it is better to set up stronger encryption with no authentication than to set up weaker encryption with the local user database.

When you select **WPA2-PSK** in your EMG1302-R10A, you can also select an option (**WPA Compatible**) to support WPA as well. In this case, if some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK** (depending on the type of wireless network login) and select the **WPA Compatible** option in the EMG1302-R10A.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every wireless client in the wireless network must have the same key.

WPS

WiFi Protected Setup (WPS) is an industry standard specification, defined by the WiFi Alliance. WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Depending on the devices in your network, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the devices. Then, they connect and set up a secure network by themselves. See how to set up a secure wireless network using WPS in the Section 6.2 on page 41.

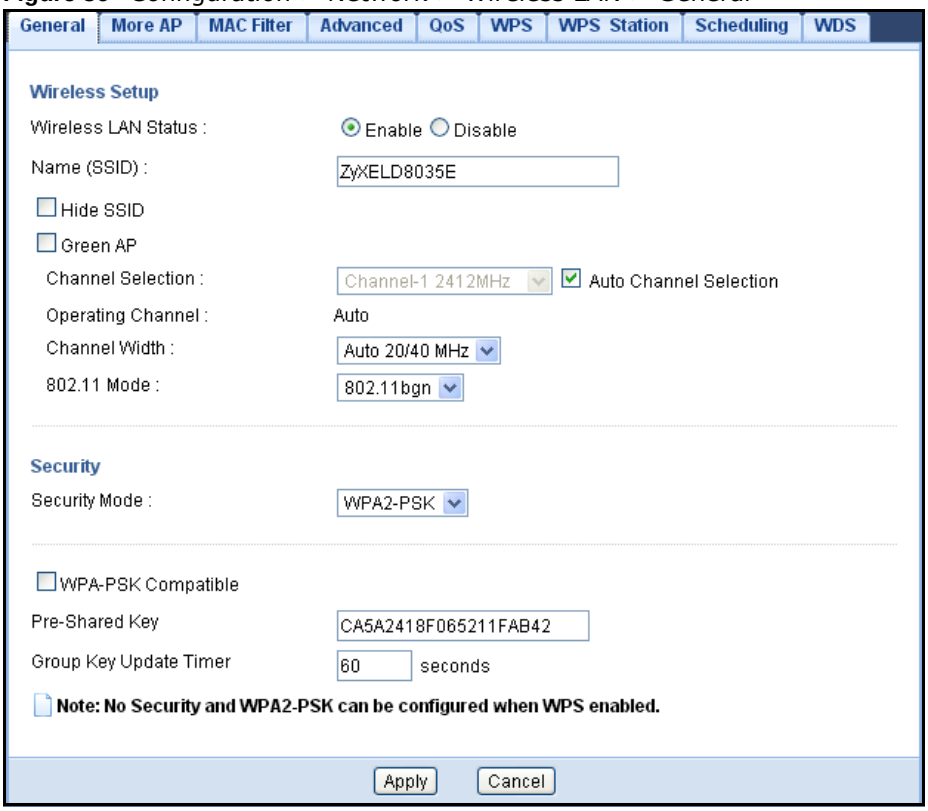
8.4 General Wireless LAN Screen

Use this screen to configure the SSID of the wireless LAN and configure the wireless security mode. The screen varies depending on what you select in the **Security Mode** field.

Note: If you are configuring the EMG1302-R10A from a computer connected to the wireless LAN and you change the EMG1302-R10A's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the EMG1302-R10A's new settings.

Click **Configuration** > **Network** > **Wireless LAN** to open the **General** screen.

Figure 36 Configuration > Network > Wireless LAN > General



The following table describes the general wireless LAN labels in this screen.

Table 20 Configuration > Network > Wireless LAN > General

LABEL	DESCRIPTION
Wireless Setup	
Wireless LAN Status	This is turned on by default. You can enable or disable the wireless LAN by using the **WLAN** switch located on the back panel of the EMG1302-R10A. The current wireless state is reflected in this field.
Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Green AP	Once Green AP is enabled, if there are no client connections to the AP, the device switches to 1T1R settings.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. This option is only available if **Auto Channel Selection** is disabled.
Auto Channel Selection	Select this check box for the EMG1302-R10A to automatically choose the channel with the least interference. Deselect this check box if you wish to manually select the channel using the **Channel Section** field.
Operating Channel	This displays the channel the EMG1302-R10A is currently using.

Table 20 Configuration > Network > Wireless LAN > General (continued)

LABEL	DESCRIPTION
Channel Width	Select whether the EMG1302-R10A uses a wireless channel width of 20MHz or **Auto**. If **Auto** is selected, the EMG1302-R10A will use 40MHz if it is supported. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. Select **20MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding. This field is available only when you set the **802.11** Mode to **802.11n** or **802.11b+g+n** in the Advanced Setup screen.
802.11 Mode	Select **802.11b** Only to allow only IEEE 802.11b compliant WLAN devices to associate with the EMG1302-R10A. Select **802.11g** Only to allow only IEEE 802.11g compliant WLAN devices to associate with the EMG1302-R10A. Select **802.11b+g** to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the EMG1302-R10A. The transmission rate of your EMG1302-R10A might be reduced. Select **802.11n** to allow only IEEE 802.11n compliant WLAN devices to associate with the EMG1302-R10A. Select **802.11g+n** to allow either IEEE 802.11g or IEEE 802.11n compliant WLAN devices to associate with the EMG1302-R10A. The transmission rate of your EMG1302-R10A might be reduced. Select **802.11b+g+n** to allow IEEE 802.11b, IEEE 802.11g or IEEE802.11n compliant WLAN devices to associate with the EMG1302-R10A. The transmission rate of your EMG1302-R10A might be reduced.
Security	
Security Mode	Choose the security mode from the drop-down list box. See Section 8.5 on page 79 for more information on wireless security settings.
WPA-PSK Compatible	This field appears when you choose **WPA2-PSK** as the **Security Mode**. Check this field to allow wireless devices using **WPA-PSK** security mode to connect to your EMG1302-R10A.
Pre-Shared Key	WPA-PSK/WPA2-PSK uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP sends a new group key out to all clients. The default is 3600 seconds (60 minutes).
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

See the rest of this chapter for information on the other labels in this screen.

8.5 Wireless Security

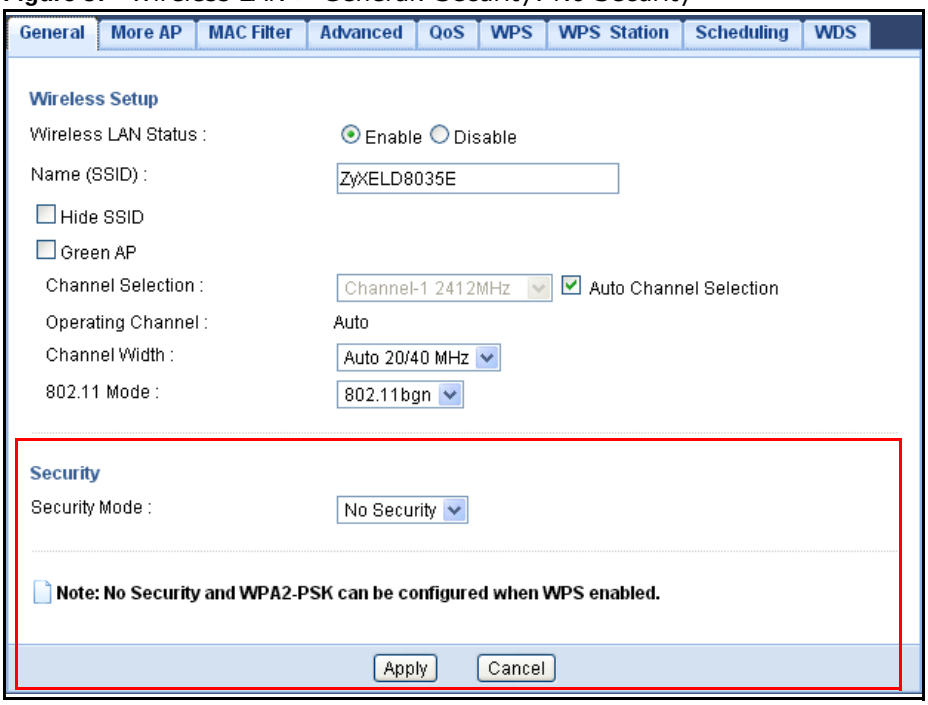
Use this part of the **General** screen to select the wireless security mode. Click **Network** > **Wireless LAN** to open the **General** screen. The screen varies depending on what you select in the **Security Mode** field.

8.5.1 No Security

Select **No Security** to allow wireless clients to communicate with the access points without any data encryption.

Note: If you do not enable any wireless security on your EMG1302-R10A, your network is accessible to any wireless network device that is within range.

Figure 37 Wireless LAN > General: Security: No Security



The following table describes the labels in this screen.

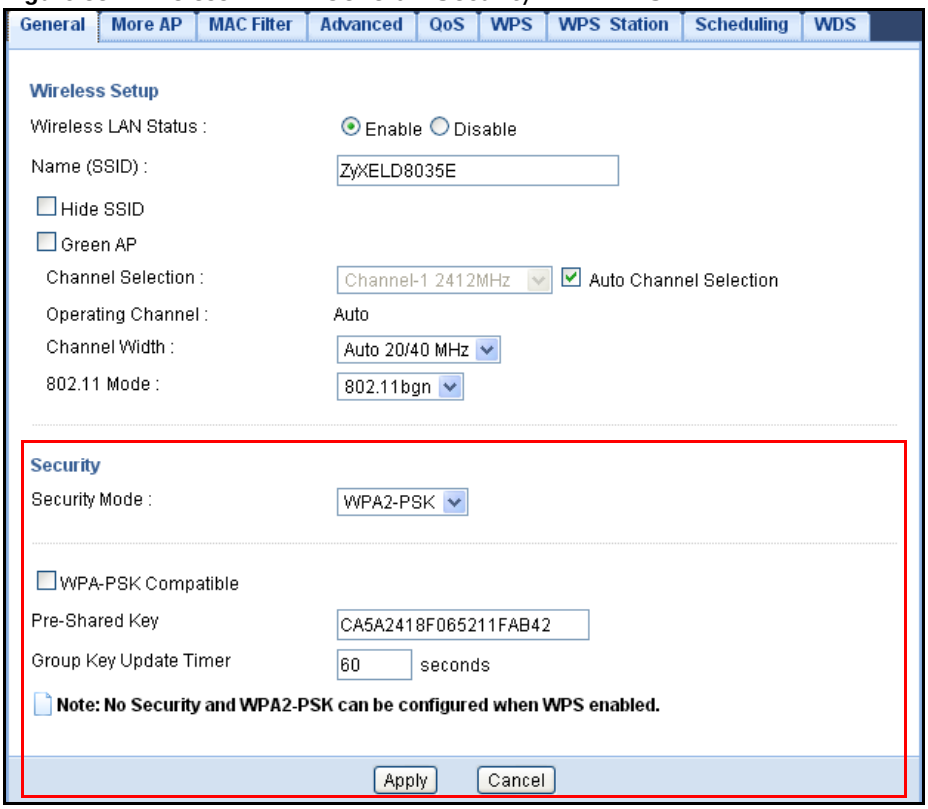
Table 21 Wireless LAN > General: Security: No Security

LABEL	DESCRIPTION
Security Mode	Choose **No Security** from the drop-down list box.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

8.5.2 WPA2-PSK

Select **WPA2-PSK** from the **Security Mode** list.

Figure 38 Wireless LAN > General: Security: WPA2-PSK



The following table describes the labels in this screen.

Table 22 Wireless LAN > General: Security: WPA-PSK/WPA2-PSK

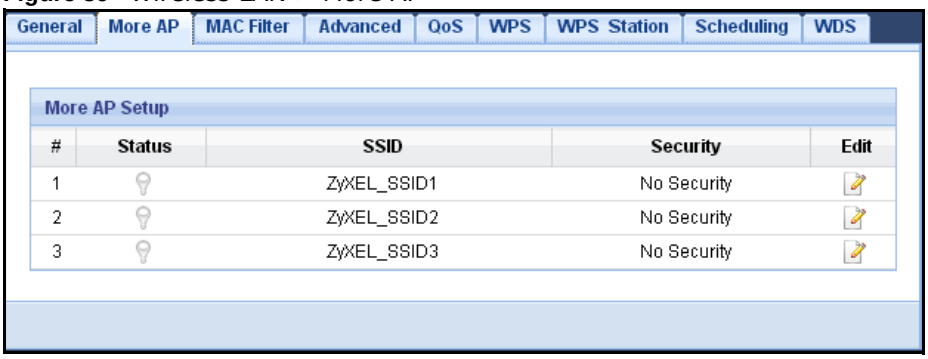
LABEL	DESCRIPTION
Security Mode	Select **WPA-PSK** or **WPA2-PSK** to enable data encryption.
WPA-PSK Compatible	This field appears when you choose **WPA2-PSK** as the **Security Mode**.
Pre-Shared Key	WPA-PSK/WPA2-PSK uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP sends a new group key out to all clients. The default is 3600 seconds (60 minutes).
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

8.6 More AP

This screen allows you to enable and configure multiple wireless networks on the EMG1302-R10A.

Select **Configuration** > **Network** > **Wireless LAN** > **More AP**. The screen appears as shown.

Figure 39 Wireless LAN > More AP



The following table describes the labels in this screen.

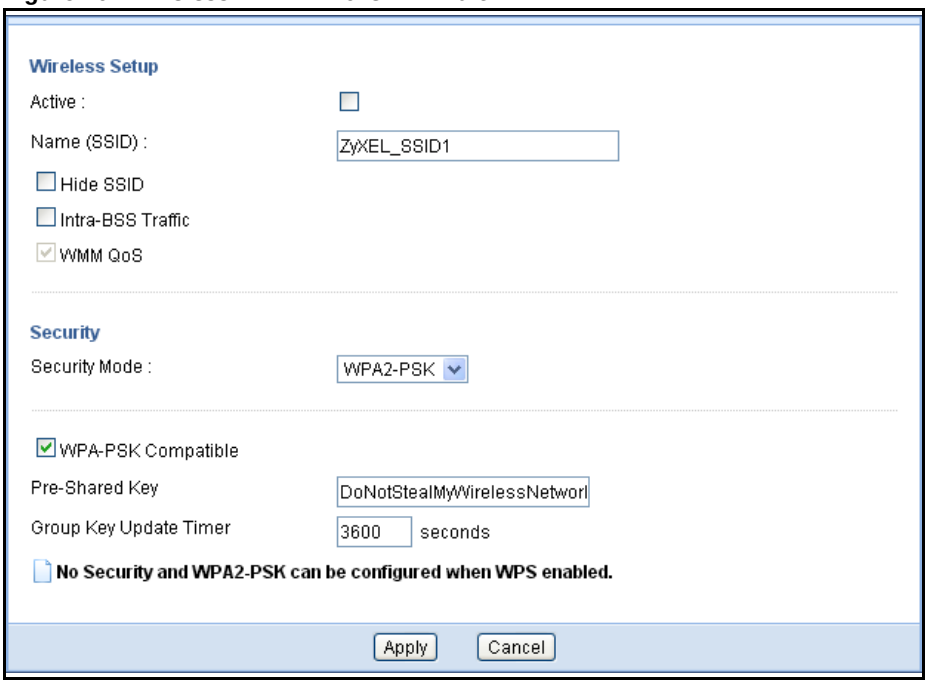
Table 23 Wireless LAN > More AP

LABEL	DESCRIPTION
#	This is the index number of each SSID profile.
Status	Shows the status of the SSID.
SSID	The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Edit	Click the **Edit** icon to configure SSID profile.

8.6.1 More AP Edit

Use this screen to edit an SSID profile. Click the **Edit** icon next to an SSID in the **Configuration** > **Network** > **Wireless LAN** > **More AP** screen. The following screen displays.

Figure 40 Wireless LAN > More AP: Edit



The following table describes the labels in this screen.

Table 24 Wireless LAN > More AP

LABEL	DESCRIPTION
Wireless Setup	
Active	Click the check box to activate wireless LAN.
Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Intra-BSS Traffic	Intra-BSS traffic is traffic between wireless stations in the BSS. Select this check box to enable **Intra-BSS Traffic**.
WMM QoS	Check this to have the EMG1302-R10A automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
Security	
Security Mode	This field indicates the security mode of the SSID profile.
WPA-PSK Compatible	This field appears when you choose **WPA2-PSK** as the Security Mode. Check this field to allow wireless devices using **WPA-PSK** security mode to connect to your ZyXEL Device.
Pre-Shared Key	Enter an 8 to 64 (case-sensitive keyboard) characters to define the pre-shared key for the security setting.

Table 24 Wireless LAN > More AP (continued)

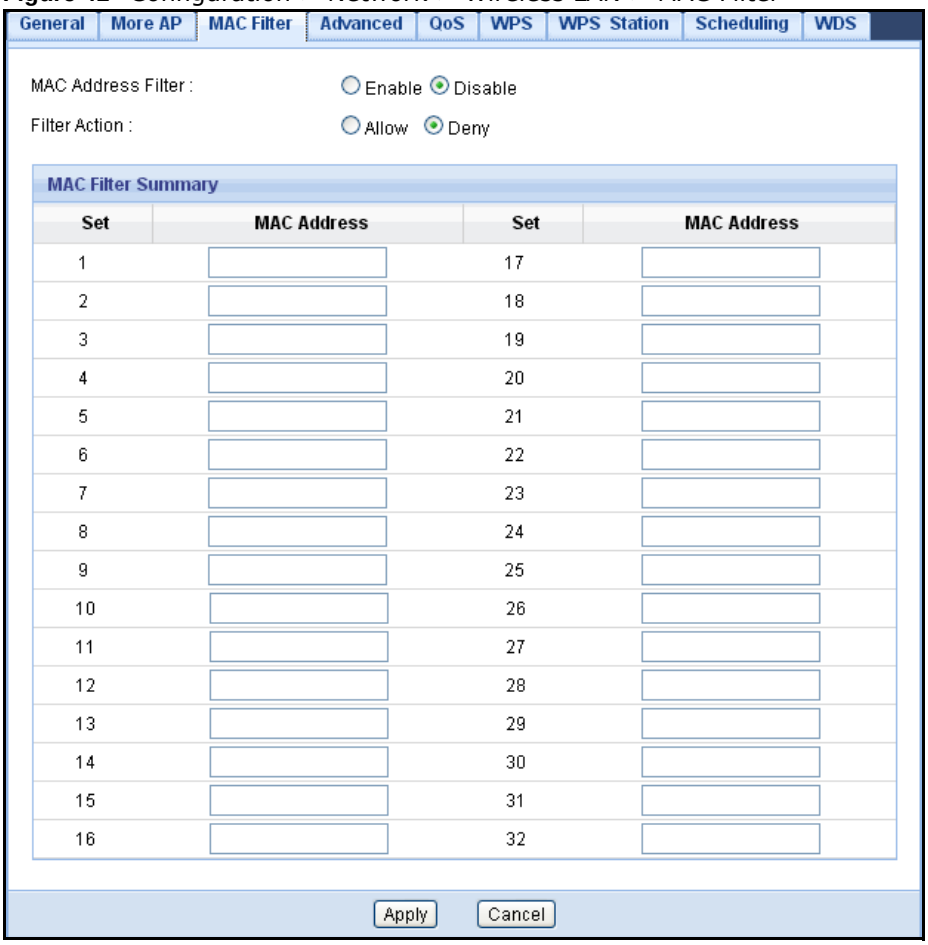
LABEL	DESCRIPTION
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the RADIUS server sends a new group key out to all clients. Note: No Security and WPA2-PSK can be configured when WPS is enabled.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

8.7 MAC Filter

The MAC filter screen allows you to configure the EMG1302-R10A to give exclusive access to devices (Allow) or exclude devices from accessing the EMG1302-R10A (Deny). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your EMG1302-R10A's MAC filter settings, click **Configuration** > **Network** > **Wireless LAN** > **MAC Filter**. The screen appears as shown.

Figure 41 Configuration > Network > Wireless LAN > MAC Filter



The following table describes the labels in this menu.

Table 25 Configuration > Network > Wireless LAN > MAC Filter

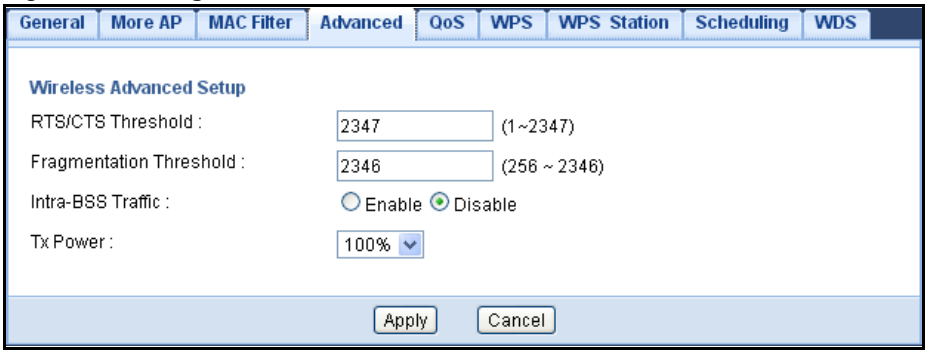
LABEL	DESCRIPTION
MAC Address Filter	Select **Disable** to deactivate the MAC filtering rule you configure below.
Filter Action	Select **Allow** to permit access to the EMG1302-R10A, MAC addresses not listed will be denied access to the EMG1302-R10A. Select **Deny** to block access to the EMG1302-R10A, MAC addresses not listed will be allowed to access the EMG1302-R10A
MAC Filter Summary	
Set	This is the index number of the MAC address.
MAC Address	This is the MAC address of the wireless station that are allowed or denied access to the EMG1302-R10A.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

8.8 Wireless LAN Advanced Screen

Use this screen to allow wireless advanced features, such as the output power, RTS/CTS Threshold and high-throughput physical mode settings.

Click **Configuration** > **Network** > **Wireless LAN** > **Advanced**. The screen appears as shown.

Figure 42 Configuration > Network > Wireless LAN > Advanced



The following table describes the labels in this screen.

Table 26 Configuration > Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
Wireless Advanced Setup	
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/ CTS (Clear To Send) handshake. Enter a value between **1** and **2347**.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between **256** and **2346**.

Table 26 Configuration > Network > Wireless LAN > Advanced (continued)

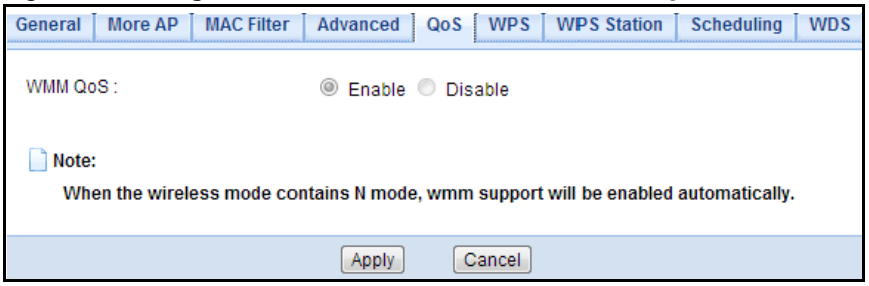
LABEL	DESCRIPTION
Intra-BSS Traffic	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.
Tx Power	Set the Tx power of the EMG1302-R10A in this field. If there is a high density of APs in an area, decrease the output power of the EMG1302-R10A to reduce interference with other APs. Select one of the following **100%**, **90%**, **75%**, **50%**, **25%** or **10%**. See the product specifications for more information on your EMG1302-R10A's output power.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

8.9 Quality of Service (QoS) Screen

The QoS screen allows you to automatically give a service (such as VoIP and video) a priority level.

Click **Configuration** > **Network** > **Wireless LAN** > **QoS**. The following screen appears.

Figure 43 Configuration > Network > Wireless LAN > QoS



The following table describes the labels in this screen.

Table 27 Configuration > Network > Wireless LAN > QoS

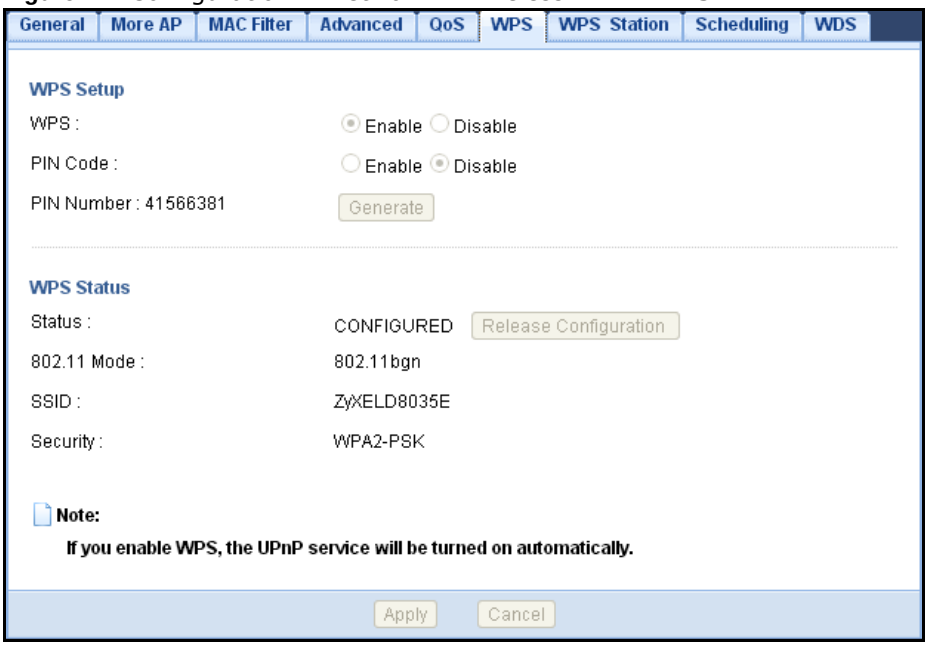
LABEL	DESCRIPTION
WMM QoS	Check **Enable** to have the EMG1302-R10A automatically give a service a priority level according to the ToS value in the IP header of packets it sends. Check **Disable** to disable the function. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
Apply	Click **Apply** to save your changes to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

8.10 WPS Screen

Use this screen to enable/disable WPS, view or generate a new PIN number and check current WPS status. To open this screen, click **Configuration** > **Network** > **Wireless LAN** > **WPS**.

Note: With WPS, wireless clients can only connect to the wireless network using the first SSID on the EMG1302-R10A.

Figure 44 Configuration > Network > Wireless LAN > WPS



The following table describes the labels in this screen.

Table 28 Configuration > Network > Wireless LAN > WPS

LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select this to enable the WPS feature.
PIN Code	Select this to enable PIN code.
PIN Number	This displays the last PIN number generated by the system, if any. Click **Generate** to generate a new PIN number.
WPS Status	
Status	This displays **Configured** when the EMG1302-R10A has connected to a wireless network using WPS or when **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there are no wireless or wireless security changes on the EMG1302-R10A or you click **Release Configuration** to remove the configured wireless and wireless security settings.
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the EMG1302-R10A.
SSID	This is the name of the wireless network (the EMG1302-R10A's first SSID).
Security	This is the type of wireless security employed by the network.

Table 28 Configuration > Network > Wireless LAN > WPS (continued)

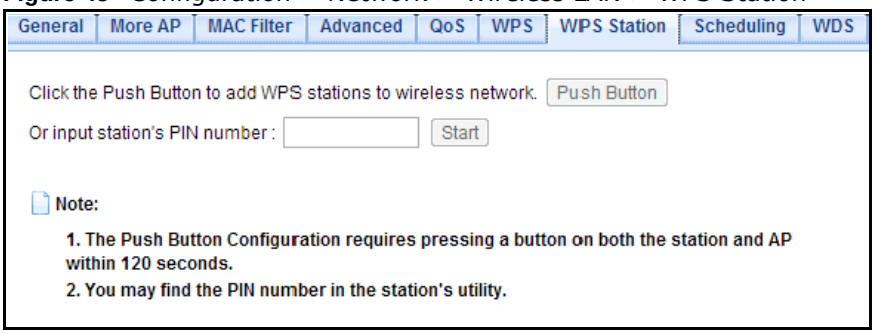
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

8.11 WPS Station Screen

Use this screen when you want to add a wireless station using WPS. To open this screen, click **Configuration** > **Network** > **Wireless LAN** > **WPS Station**.

Note: After you click **Push Button** on this screen, you have to press a similar button in the wireless station utility within 2 minutes. To add the second wireless station, you have to press these buttons on both device and the wireless station again after the first 2 minutes.

Figure 45 Configuration > Network > Wireless LAN > WPS Station



The following table describes the labels in this screen.

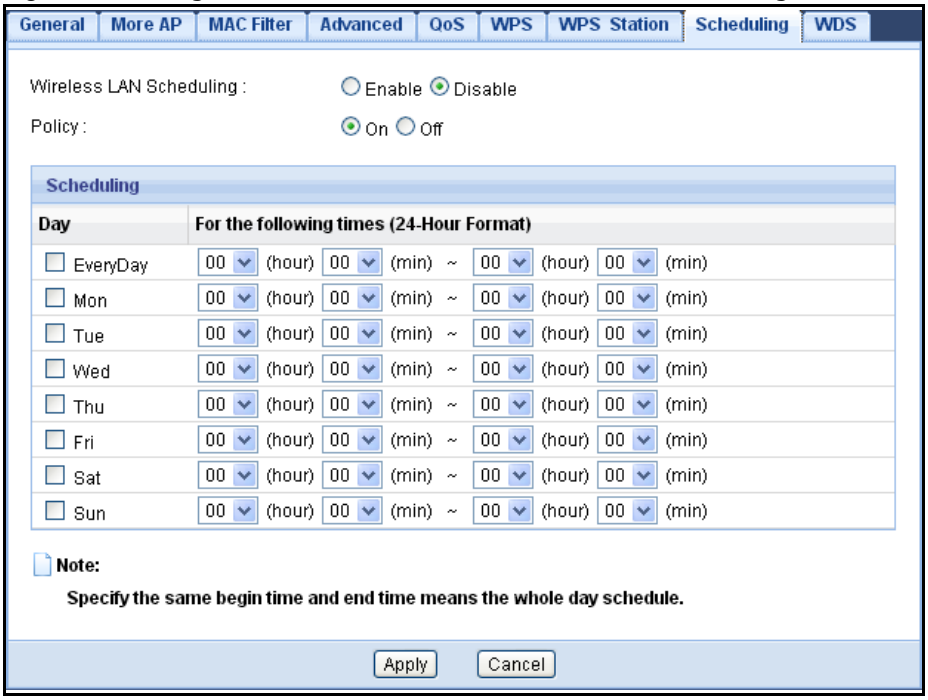
Table 29 Configuration > Network **>** Wireless LAN > WPS Station

LABEL	DESCRIPTION
Push Button	Use this button when you use the PBC (Push Button Configuration) method to configure wireless stations's wireless settings. Click this to start WPS-aware wireless station scanning and the wireless security information synchronization.
Or input station's PIN number	Use this button when you use the PIN Configuration method to configure wireless station's wireless settings. Type the same PIN number generated in the wireless station's utility. Then click **Start** to associate to each other and perform the wireless security information synchronization.

8.12 Scheduling Screen

Use this screen to set the times your wireless LAN is turned on and off. Wireless LAN scheduling is disabled by default. The wireless LAN can be scheduled to turn on or off on certain days and at certain times. To open this screen, click **Configuration** > **Network > Wireless LAN** > **Scheduling**.

Figure 46 Configuration > Network **>** Wireless LAN > Scheduling



The following table describes the labels in this screen.

Table 30 Configuration > Network **>** Wireless LAN > Scheduling

LABEL	DESCRIPTION
Enable Wireless LAN Scheduling	Select this to enable Wireless LAN scheduling.
Policy	Select **On** to activate the selected schedule. Select **Off** to deactivate the selected schedule.
Scheduling	
Day	Select **Everyday** or the specific days to turn the Wireless LAN on or off. If you select **Everyday** you can not select any specific days. This field works in conjunction with the **For the following times** field.
For the following times (24-Hour Format)	Select a begin time using the first set of **hour** and minute (**min**) drop down boxes and select an end time using the second set of **hour** and minute (**min**) drop down boxes. If you have chosen **On** earlier for the WLAN Status the Wireless LAN will turn on between the two times you enter in these fields. If you have chosen **Off** earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

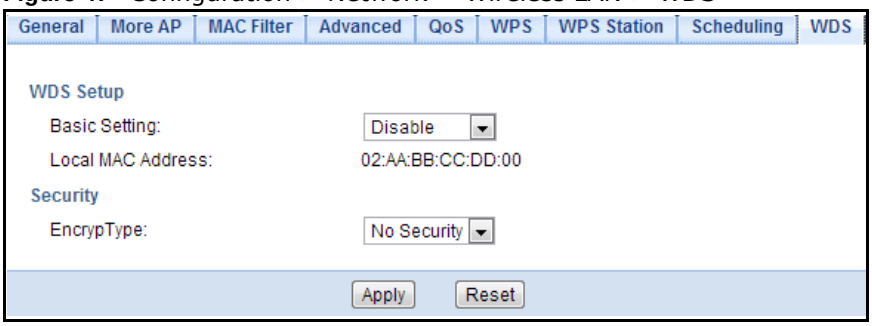
8.13 WDS

A Wireless Distribution System is a wireless connection between two or more APs. Use this screen to set the operating mode of your EMG1302-R10A to **AP + Bridge** or **Bridge Only** and establish wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode.

Note: You must enable the same wireless security settings on the EMG1302-R10A and on all wireless clients that you want to associate with it.

To open this screen, click **Configuration** > **Network > Wireless LAN** > **WDS**.

Figure 47 Configuration > Network **>** Wireless LAN > WDS



The following table describes the labels in this screen.

Table 31 Configuration > Network **>** Wireless LAN > WDS

LABEL	DESCRIPTION
WDS Setup	
Basic Settings	Select the operating mode for your EMG1302-R10A. • **AP + Bridge** - The EMG1302-R10A functions as a bridge and access point simultaneously. • **Bridge Only** - The EMG1302-R10A acts as a wireless network bridge and establishes wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode. The EMG1302-R10A can establish up to five wireless links with other APs.
Local MAC Address	This is the MAC address of your EMG1302-R10A.
PHY Mode (Bridge only)	Select CCK (11b mode), OFDM (11g mode), HTMIX (11b/g/n mixed mode) or GREENFIELD (11n mode) from the drop-down menu. All AP devices should be setup to the same Phy mode.
Remote MAC Address (AP+Bridge / Bridge only)	This is the MAC address of a remote device.
Security	
EncrypType	Select whether to use **TKIP** or **AES** encryption for your **WDS** connection in this field. Otherwise, select **No Security**.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Reset	Click **Reset** to reload the previous configuration for this screen.

9

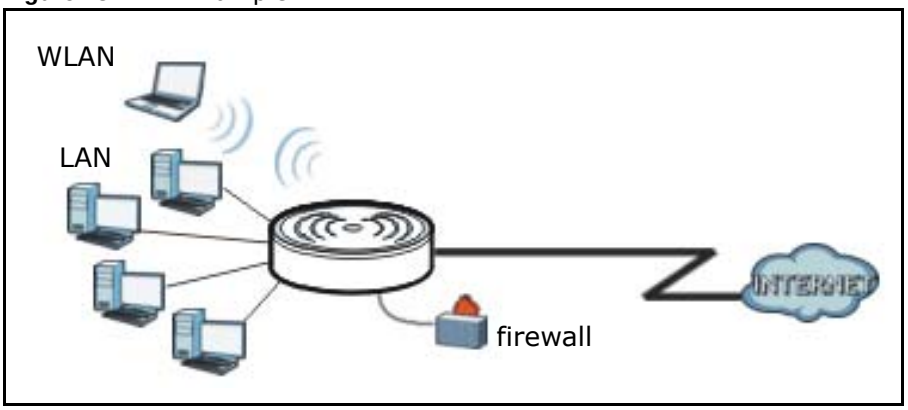
LAN

9.1 Overview

This chapter describes how to configure LAN settings.

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

Figure 48 LAN Example



The LAN screens can help you manage IP addresses.

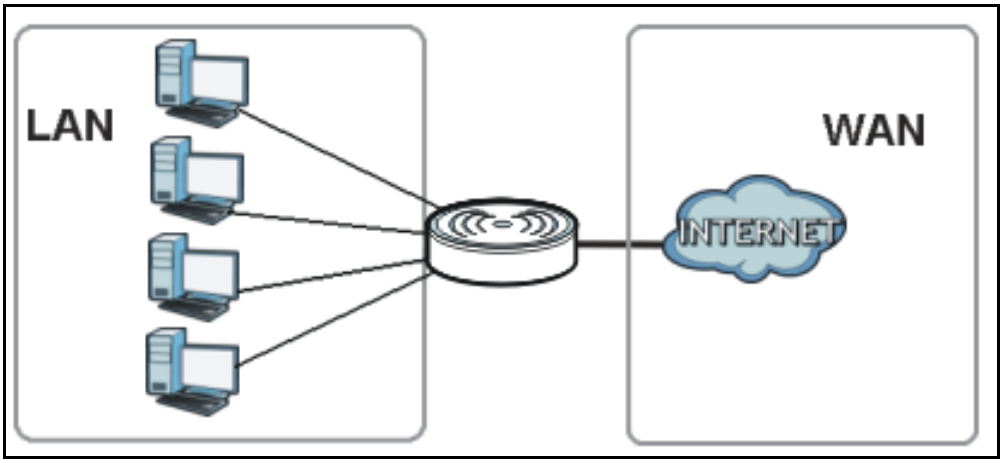
9.2 What You Can Do

- Use the **IP** screen to change the IP address for your EMG1302-R10A (Section 9.4 on page 93).

9.3 What You Need To Know

The actual physical connection determines whether the EMG1302-R10A ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 49 LAN and WAN IP Addresses



The LAN parameters of the EMG1302-R10A are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded Web Configurator help regarding what fields need to be configured.

9.3.1 IP Pool Setup

The EMG1302-R10A is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the EMG1302-R10A itself) in the lower range (192.168.1.2 to 192.168.1.32) for other server computers, for instance, servers for mail, T, web, etc., that you may have.

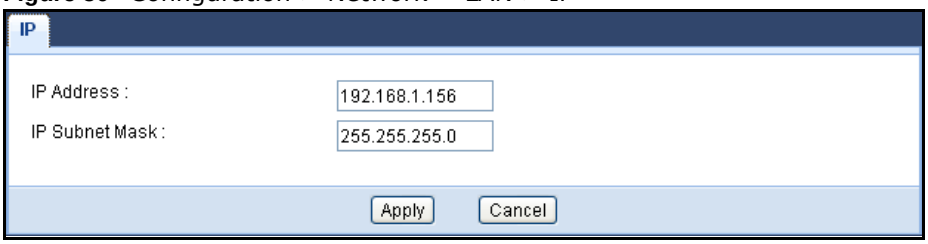
9.3.2 LAN TCP/IP

The EMG1302-R10A has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

9.4 LAN IP Screen

Use this screen to change the IP address for your EMG1302-R10A. Click **Configuration > Network > LAN > IP**.

Figure 50 Configuration > Network > LAN > IP



The following table describes the labels in this screen.

Table 32 Configuration > Network > LAN > IP

LABEL	DESCRIPTION
IP Address	Type the IP address of your EMG1302-R10A in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your EMG1302-R10A will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the EMG1302-R10A.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10

DHCP Server

10.1 Overview

Dynamic Host Configuration Protocol (DHCP), RFC 2131 and RFC 2132 allow individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the EMG1302-R10A's LAN as a DHCP server or disable it. When configured as a server, the EMG1302-R10A provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

10.2 What You Can Do

- Use the **General** screen to enable the DHCP server (Section 10.4 on page 96).
- Use the **Advanced** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses (Section 10.5 on page 97).
- Use the **Client List** screen to view DHCP client list (Section 10.6 on page 98).

10.3 What You Need To Know

The following terms and concepts may help as you read through this chapter.

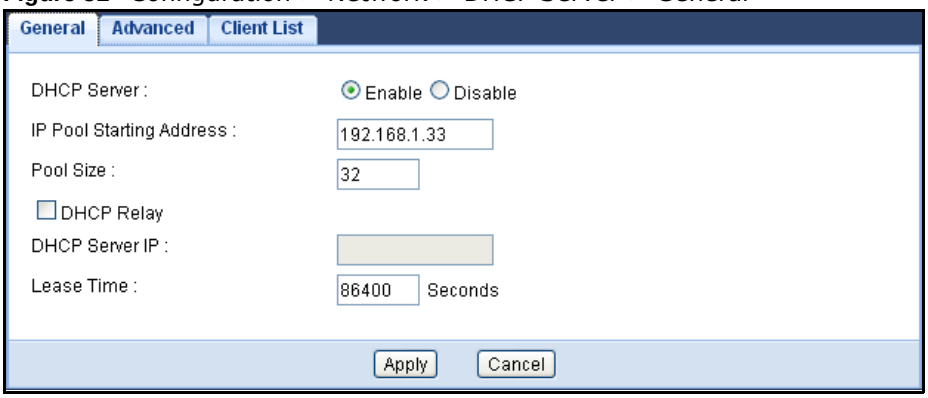
MAC Addresses

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. Find out the MAC addresses of your network devices if you intend to add them to the **DHCP Client List** screen.

10.4 The DHCP General Screen

Use this screen to enable the DHCP server. Click **Configuration** > **Network** > **DHCP Server**. The **General** screen displays.

Figure 51 Configuration > Network > DHCP Server > General



The following table describes the labels in this screen.

Table 33 Configuration > Network > DHCP Server > General

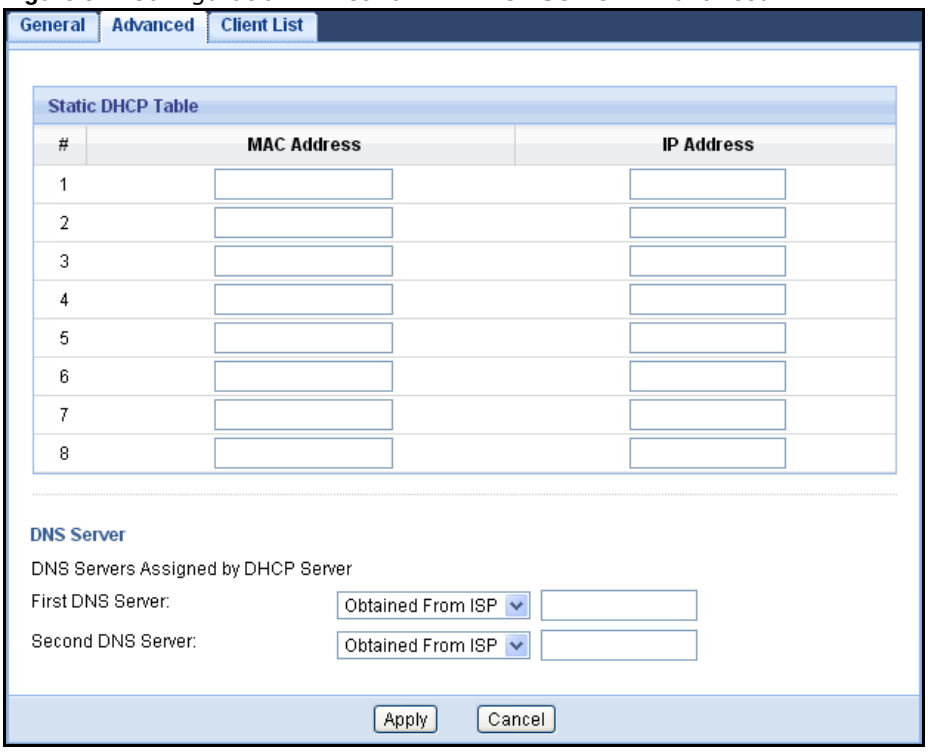
LABEL	DESCRIPTION
Enable DHCP Server	Select the checkbox to enable DHCP for LAN. DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Leave the **Enable DHCP Server** check box selected unless your ISP instructs you to do otherwise. Clear it to disable the EMG1302-R10A acting as a DHCP server. When configured as a server, the EMG1302-R10A provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool for LAN.
Pool Size	This field specifies the size, or count of the IP address pool for LAN.
DHCP Relay	Select the checkbox to enable DHCP relay and forward a DHCP request to the DHCP server.
DHCP Server IP	Enter the IP address of the DHCP server.
Lease Time	Enter the in seconds the designated lease time for a DHCP assignment.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10.5 The DHCP Advanced Screen

This screen allows you to assign IP addresses on the LAN to specific individual computers based on their MAC addresses. You can also use this screen to configure the DNS server information that the EMG1302-R10A sends to the DHCP clients.

To change your EMG1302-R10A's static DHCP settings, click **Configuration** > **Network** > **DHCP Server** > **Advanced**. The following screen displays.

Figure 52 Configuration > Network > DHCP Server > Advanced



The following table describes the labels in this screen.

Table 34 Configuration > Network > DHCP Server > Advanced

LABEL	DESCRIPTION
Static DHCP Table	
#	This is the index number of the static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	Type the LAN IP address of a computer on your LAN.
DNS Server	
DNS Servers Assigned by DHCP Server	The EMG1302-R10A passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The EMG1302-R10A only passes this information to the LAN DHCP clients when you select the **Enable DHCP Server** check box. When you clear the **Enable DHCP Server** check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.

Table 34 Configuration > Network > DHCP Server > Advanced (continued)

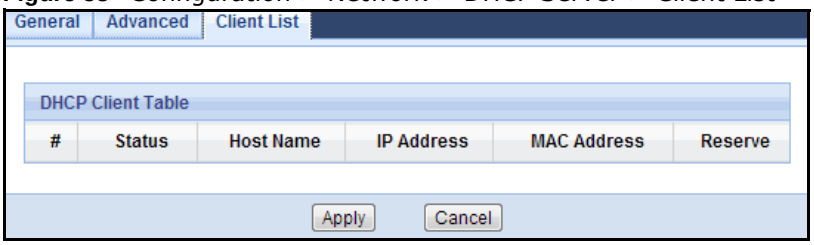
LABEL	DESCRIPTION
First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the EMG1302-R10A's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **DNS Relay** to have the EMG1302-R10A act as a DNS proxy. The EMG1302-R10A's LAN IP address displays in the field to the right (read-only). The EMG1302-R10A tells the DHCP clients on the LAN that the EMG1302-R10A itself is the DNS server. When a computer on the LAN sends a DNS query to the EMG1302-R10A, the EMG1302-R10A forwards the query to the EMG1302-R10A's system DNS server (configured in the **WAN > Internet Connection** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select **DNS Relay** for a second or third DNS server, that choice changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10.6 The DHCP Client List Screen

This screen allows you to review the list of the devices currently connected to the EMG1302-R10A.

To view your EMG1302-R10A's DHCP client list, click **Configuration** > **Network** > **DHCP Server** > **Client List**. The following screen displays.

Figure 53 Configuration > Network > DHCP Server > Client List



The following table describes the labels in this screen.

Table 35 Configuration > Network > DHCP Server > Client List

LABEL	DESCRIPTION
DHCP Client Table	
#	This is the index number of the client device.
Status	This shows the status of the connected device.
Host Name	This indicates the device's host name.
IP Address	This indicates the IP address assigned to this client device.

Table 35 Configuration > Network > DHCP Server > Client List (continued)

LABEL	DESCRIPTION
MAC Address	Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. This indicates the MAC address of the client device.
Reserve	Select this if you want to reserve the IP address for this specific MAC address.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11

Quality of Service (QoS)

11.1 Overview

Use the **QoS** screen to set up your EMG1302-R10A to use QoS for traffic management.

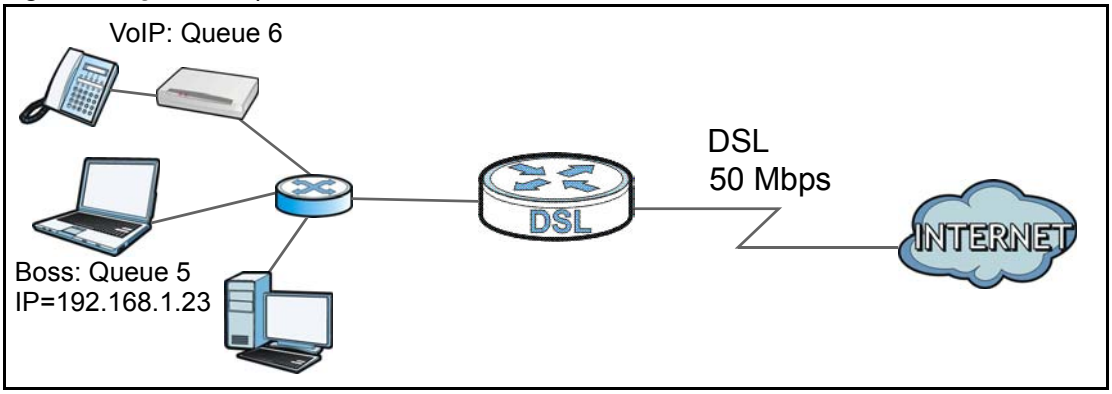
Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control bandwidth. QoS allows the EMG1302-R10A to group and prioritize application traffic and fine-tune network performance.

Without QoS, all traffic data are equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical applications such as video-on-demand.

The EMG1302-R10A assigns each packet a priority and then queues the packet accordingly. Packets assigned with a high priority are processed more quickly than those with low priorities if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

In the following figure, your Internet connection has an upstream transmission speed of 50 Mbps. You configure a classifier to assign the highest priority queue (6) to VoIP traffic from the LAN interface, so that voice traffic would not get delayed when there is network congestion. Traffic from the boss's IP address (192.168.1.23 for example) is mapped to queue 5. Traffic that does not match these two classes are assigned priority queue based on the internal QoS mapping table on the EMG1302-R10A.

Figure 54 QoS Example



11.1.1 What You Can Do in the QoS Screens

- Use the **General** screen (Section 11.2 on page 102) to enable QoS on the EMG1302-R10A, and specify the type of scheduling.
- Use the **Rule-based QoS** screen (Section 11.3 on page 103) to define and setup QoS-specific rules.

11.1.2 What You Need to Know About QoS

802.1p

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. 802.1p is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use 802.1p to give different priorities to different packet types.

Tagging and Marking

In a QoS class, you can configure whether to add or change the DiffServ Code Point (DSCP) value and IEEE 802.1p priority level in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

Finding Out More

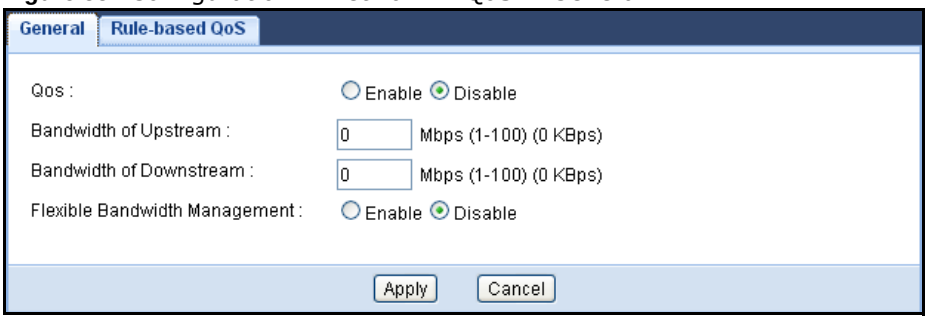
See Section 11.4 on page 105 for advanced technical information on QoS.

11.2 The Quality of Service General Screen

Use this screen to enable or disable QoS and set the upstream bandwidth.

Click **Configuration > Network > QoS > General** to open the screen as shown next.

Figure 55 Configuration > Network > QoS > General



The following table describes the labels in this screen.

Table 36 Configuration > Network > QoS > General

LABEL	DESCRIPTION
QoS	Select **Enable** or **Disable** to activate/disable the service.
Bandwidth of Upstream	Enter the amount of upstream bandwidth for the WAN interfaces that you want to allocate using QoS. The recommendation is to set this speed to match the interfaces' actual transmission speed. For example, set the WAN interfaces' speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps. You can set this number higher than the interfaces' actual transmission speed. The ZyXEL Device uses up to 95% of the DSL port's actual upstream transmission speed even if you set this number higher than the DSL port's actual transmission speed. You can also set this number lower than the interfaces' actual transmission speed. This will cause the ZyXEL Device to not use some of the interfaces' available bandwidth. If you leave this field blank, the ZyXEL Device automatically sets this number to be 95% of the WAN interfaces' actual upstream transmission speed.
Bandwidth of Downstream	Enter the amount of downstream bandwidth for the LAN interfaces (including HPNA and WLAN) that you want to allocate using QoS. The recommendation is to set this speed to match the WAN interfaces' actual transmission speed. For example, set the LAN managed downstream bandwidth to 100000 kbps if you use a 100 Mbps wired Ethernet WAN connection. You can also set this number lower than the WAN interfaces' actual transmission speed. This will cause the ZyXEL Device to not use some of the interfaces' available bandwidth. If you leave this field blank, the ZyXEL Device automatically sets this to the LAN interfaces' maximum supported connection speed.
Flexible Bandwidth Management	Select **Enable** or **Disable** to activate/disable the service.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.3 The Rule-based QoS Screen

Click **Configuration > Network > QoS > Queue** to open the screen as shown next.

Figure 56 Configuration > Network > QoS > Queue

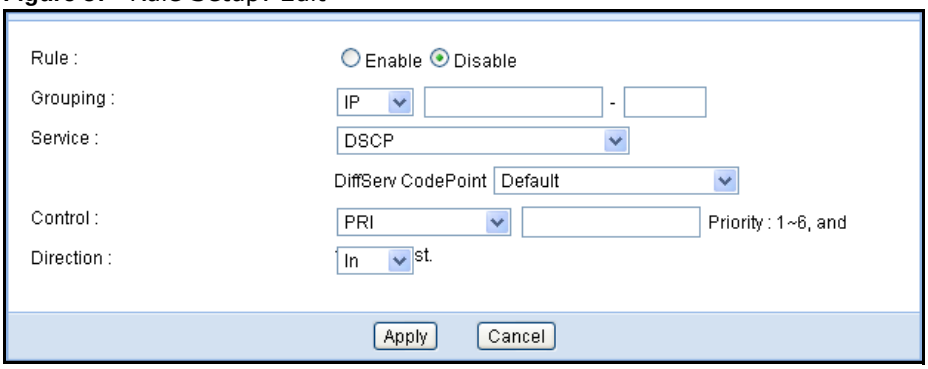
The following table describes the labels in this screen.

Table 37 Configuration > Network > QoS > Queue

LABEL	DESCRIPTION
#	This is the index number of the entry.
Status	This field displays whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Grouping	This field displays the IP or MAC interface this rule uses.
Control	This field displays the priority designation: 1 to 6 (1 is highest priority).
Direction	This field displays the direciton of the traffic (In / Out / Both) for this rule.
Modify	Click the **Edit** icon to edit the queue. Click the **Delete** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.
Restart	Click **Restart** to reset the QoS rules without requiring a device reboot.
Reset QoS Rule	Click **Reset QoS Rule** to have the rules reset at device reboot.

11.3.1 Adding a Rule

Figure 57 Rule Setup: Edit



The following table describes the labels in this screen.

Table 38 Rule Setup: Edit

LABEL	DESCRIPTION
Rule	
Grouping	Select IP to set an IP address grouping designation for this rule. Select MAC to set a MAC address grouping designation for this rule.
Service	Select **DSCP** from the drop-down menu, and select the DiffServ CodePoint in the following field. Select **Service Port** from the drop-down menu, then enter the beginning and ending port and the protocol type (TCP/UDP) in the following field. Select **Pre-defined Application profiles** from the drop-down menu, and select the corresponding Service Type in the following field. Select **Connection Sessions** from the drop-down menu, and enter the control session designation (1 to 20,000) in the following field.

Table 38 Rule Setup: Edit (continued)

LABEL	DESCRIPTION
Control	
Direction	Select the direciton of the traffic (In / Out / Both) for this rule.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.4 QoS Technical Reference

This section provides some technical background information about the topics covered in this chapter.

11.4.1 IEEE 802.1p

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 39 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for "spare bandwidth".
Level 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

11.4.2 IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

11.4.3 Automatic Priority Queue Assignment

If you enable QoS on the EMG1302-R10A, the EMG1302-R10A can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the EMG1302-R10A. On the EMG1302-R10A, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

Table 40 Internal Layer2 and Layer3 QoS Mapping

PRIORITY QUEUE	LAYER 2	LAYER 3		
	IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY)	TOS (IP PRECEDENCE)	DSCP	IP PACKET LENGTH (BYTE)
0	1	0	000000	
1	2			
2	0	0	000000	>1100
3	3	1	001110 001100 001010 001000	250~1100
4	4	2	010110 010100 010010 010000	
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000	
		7	111000	

12 NAT

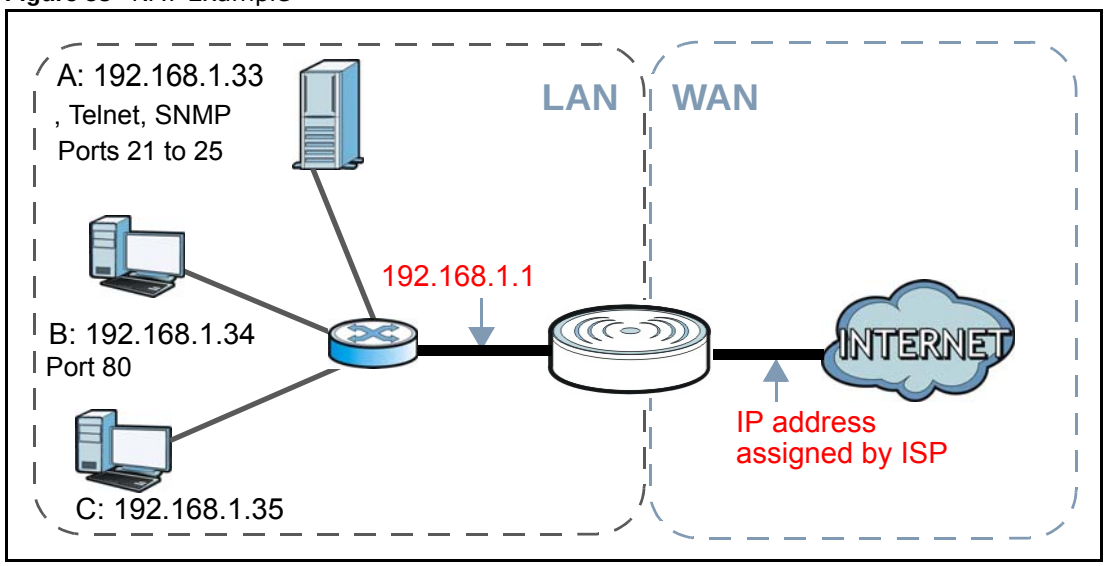
12.1 Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

The figure below is a simple illustration of a NAT network. You want to assign ports 21-25 to one, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example).

You assign the LAN IP addresses to the devices (**A** to **D**) connected to your EMG1302-R10A. The ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet. All traffic coming from **A** to **D** going out to the Internet use the IP address of the EMG1302-R10A, which is 192.168.1.1.

Figure 58 NAT Example



This chapter discusses how to configure NAT on the EMG1302-R10A.

Note: You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the EMG1302-R10A.

12.2 What You Can Do

- Use the **General** screen to enable NAT (Section 12.4 on page 110).

- Use the **Port Forwarding** screen to change your EMG1302-R10A's port forwarding settings (Section 12.5 on page 110).
- Use the **Port Trigger** screen to view and configure your EMG1302-R10A's trigger port settings (Section 12.5 on page 110).
- Use the **ALG** screen to

12.3 What You Need To Know

The following terms and concepts may help as you read through this chapter.

Inside/Outside

This denotes where a host is located relative to the EMG1302-R10A, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/Local

This denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note: Inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet.

An inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 41 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

Note: NAT never changes the IP address (either local or global) of an outside host.

What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside

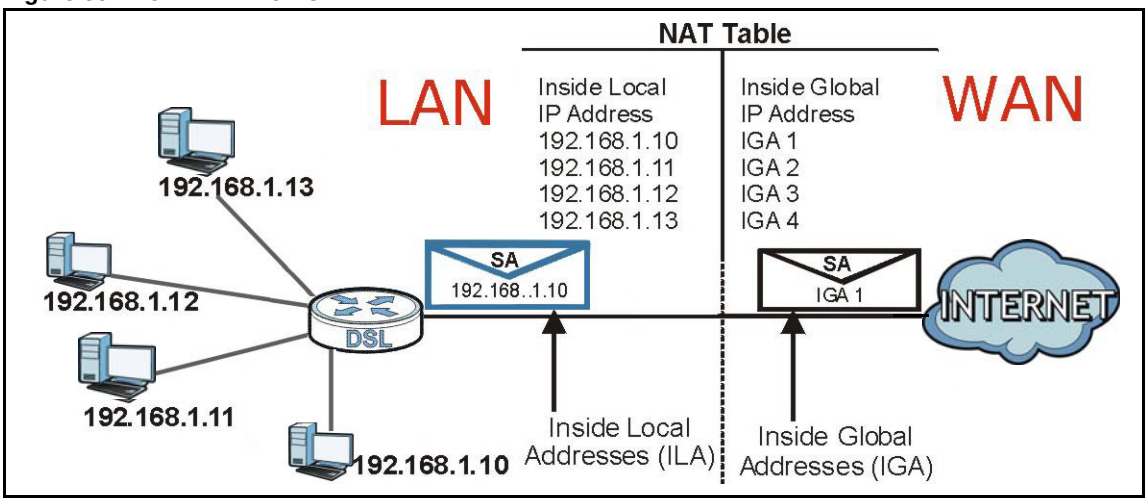
global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. With no servers defined, your EMG1302-R10A filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address in each packet and then forwards it to the Internet. The EMG1302-R10A keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

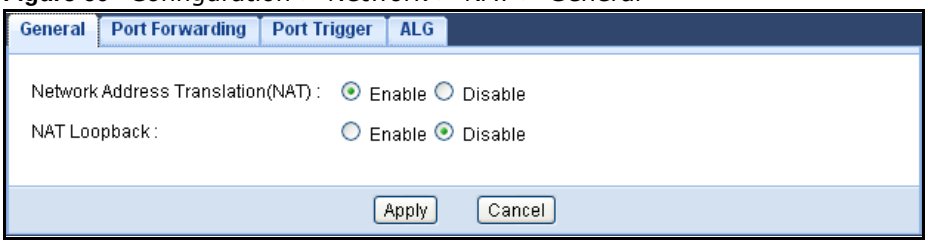
Figure 59 How NAT Works



12.4 The NAT General Screen

Use this screen to enable NAT and set a default server. Click **Configuration > Network** > **NAT** to open the **General** screen.

Figure 60 Configuration > Network > NAT > General



The following table describes the labels in this screen.

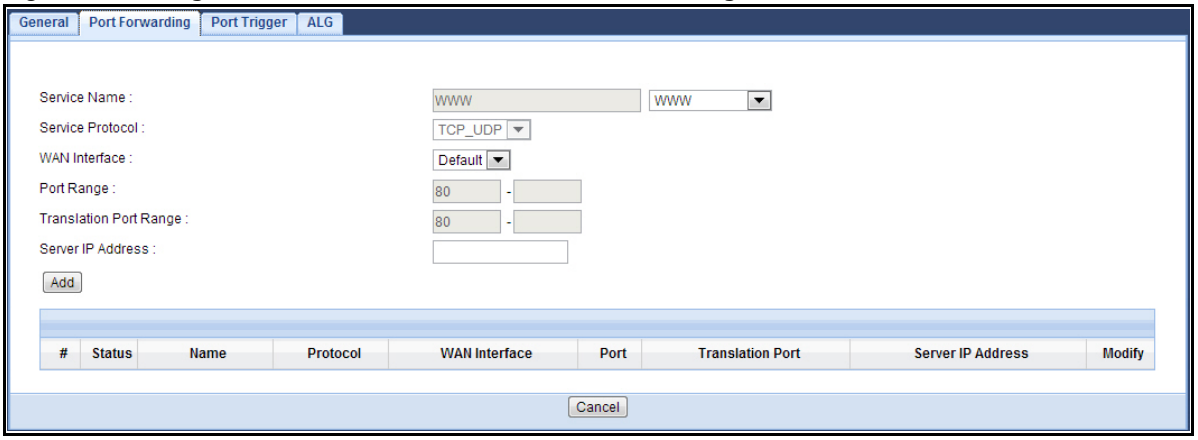
Table 42 Configuration > Network > NAT > General

LABEL	DESCRIPTION
Network Address Translation(NAT)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select the check box to enable NAT.
NAT Loopback	
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Reset	Click **Reset** to begin configuring this screen afresh.

12.5 The NAT Port Forwarding Screen

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. This screen allows you to create or edit a port forwarding rule. To change your EMG1302-R10A's NAT port forwarding settings, click **Configuration > Network** > **NAT** > **Port Forwarding**. The screen appears as shown.

Figure 61 Configuration > Network > NAT > Port Forwarding



The following table describes the labels in this screen.

Table 43 Configuration > Network > NAT > Port Forwarding

LABEL	DESCRIPTION
Service Name	Select **User-Defined** and type a name (of up to 31 printable characters) to identify this rule in the first field next to **Service Name**. Otherwise, select a predefined service in the second field next to **Service Name**. The predefined service name and port number(s) will display in the **Service Name** and **Port** fields.
Service Protocol	Select the protocol supported by this service. Choices are **TCP_UDP**, **TCP**, or **UDP**.
WAN Interface	Select a WAN interface for which you want to configure port forwarding rules.
Port Range	Type the first and last internal port number that identifies a service.
Translation Port Range	Type the first and last external port number that identifies a service.
Server IP Address	Type the inside IP address of the virtual server here.
Add	Click **Add** to save the port forwarding rule.
#	This is the number of an individual port forwarding server entry.
Status	Shows the rule status.
Name	This field displays a name to identify this rule.
Protocol	This is the protocol used by this service.
WAN Interface	This is the WAN interface of the rule.
WAN IP	This is the WAN IP address of the incoming packets.
Port	This is the internal port number that identifies the service.
Translation Port Range	Type the first and last external port number that identifies a service.
Server IP Address	This field displays the inside IP address of the server.
Modify	Click the **Edit** icon to display and modify an existing rule setting. Click the **Remove** icon to delete a rule.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

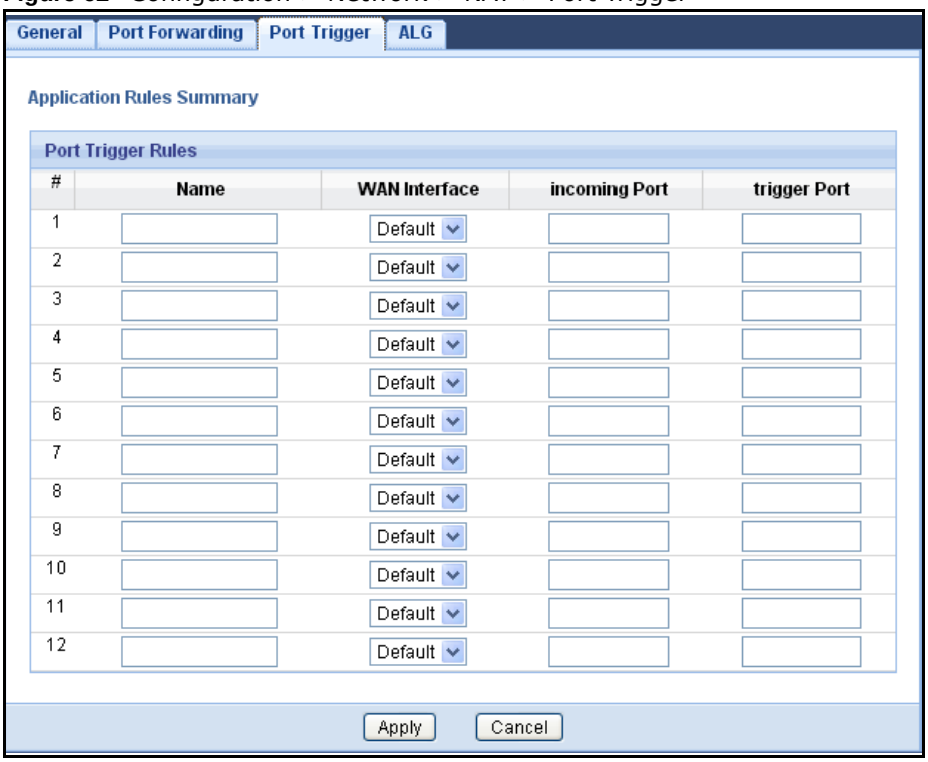
12.6 The NAT Trigger Port Screen

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The EMG1302-R10A records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the EMG1302-R10A WAN port receives a response with a specific port number and protocol ("open" port), the EMG1302-R10A forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

Use this screen to view and configure your EMG1302-R10A's trigger port settings. Click **Configuration > Network** > **NAT > Port Trigger** to open the **Port Trigger** screen.

Figure 62 Configuration > Network > NAT > Port Trigger



The following table describes the labels in this screen.

Table 44 Configuration > Network > NAT > Port Trigger

LABEL	DESCRIPTION
Application Rules Summary	
Port Trigger Rules	
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
WAN Interface	This is the WAN interface of the rule.
Incoming Port	**Incoming Port** is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The device forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Trigger Port	The trigger port is a port (or a range of ports) that causes (or triggers) the device to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

12.7 The ALG Screen

Click **Configuration > Network** > **NAT** > **ALG**. The screen appears as shown.

Figure 63 Configuration > Network > NAT > ALG

The following table describes the labels in this screen.

Table 45 Configuration > Network > NAT > ALG

LABEL	DESCRIPTION
ALG-SIP	
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13

DDNS

13.1 Overview

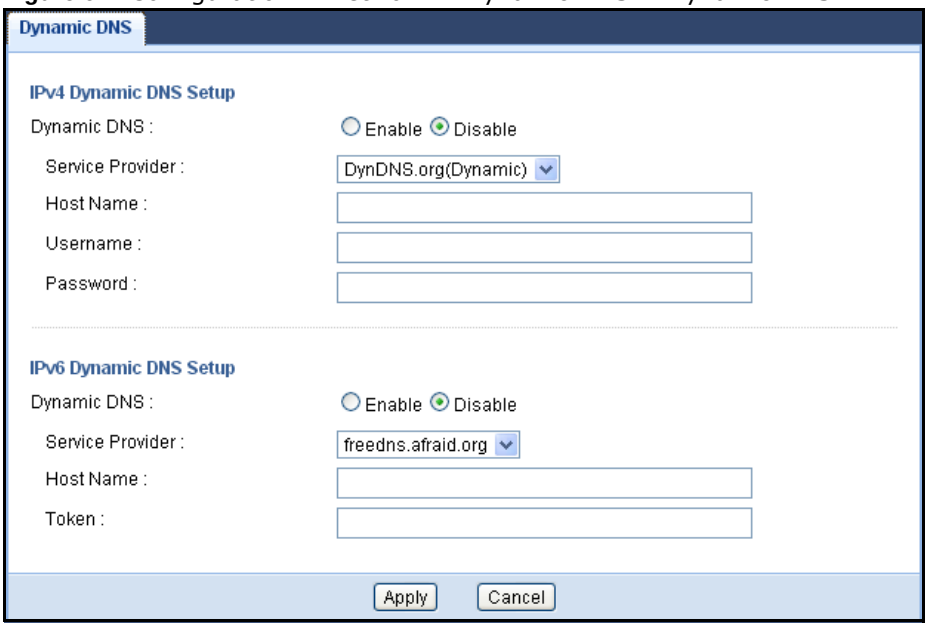
Dynamic Domain Name Service (DDNS) services let you use a fixed domain name with a dynamic IP address. Users can always use the same domain name instead of a different dynamic IP address that changes each time to connect to the EMG1302-R10A or a server in your network.

Note: The EMG1302-R10A must have a public global IP address and you should have your registered DDNS account information on hand.

13.2 The DDNS General Screen

To change your EMG1302-R10A's DDNS, click **Configuration > Network** > **DDNS**. The **General** screen appears as shown.

Figure 64 Configuration > Network > Dynamic DNS > Dynamic DNS



The following table describes the labels in this screen.

Table 46 Configuration > Network > Dynamic DNS > Dynamic DNS

LABEL	DESCRIPTION
IPv4 Dynamic DNS Setup	
Dynamic DNS	Select **Enable** to use dynamic DNS.

Table 46 Configuration > Network > Dynamic DNS > Dynamic DNS (continued)

LABEL	DESCRIPTION
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	The host name is the domain name that the DDNS service will map to your dynamic global IP address. Type the host name fully qualified, for example, 'yourhost.mydomain.net'. You can specify up to two host names in the field separated by a comma (",").
User Name	Type the user name that you used when you registered with the DDNS service.
Password	Type the password associated with the DDNS user name.
IPv6 Dynamic DNS Setup	
Dynamic DNS	Select **Enable** to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	The host name is the domain name that the DDNS service will map to your dynamic global IP address. Type the host name fully qualified, for example, 'yourhost.mydomain.net'. You can specify up to two host names in the field separated by a comma (",").
Token	This is the token authentication provided by the hosting provider (i.e. FreeDDNS). When the host name is registered, the hosting server provides the token identifier.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

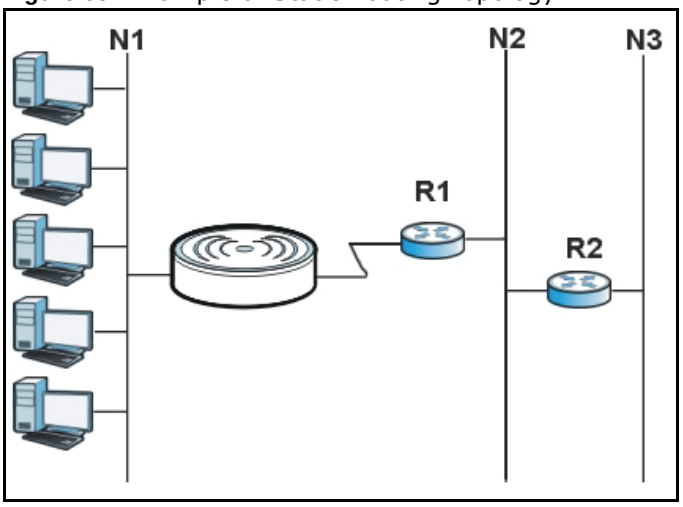
14 Routing

14.1 Overview

This chapter shows you how to configure static routes for your EMG1302-R10A.

Each remote node specifies only the network to which the gateway is directly connected, and the EMG1302-R10A has no knowledge of the networks beyond. For instance, the EMG1302-R10A knows about network N2 in the following figure through remote node Router 1. However, the EMG1302-R10A is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the EMG1302-R10A about the networks beyond the remote nodes.

Figure 65 Example of Static Routing Topology



14.2 Static Route Screen

Click **Configuration > Network > Rounting > Static Route** to open the **Static Route** screen.

Figure 66 Configuration > Network > Routing > Static Route

The following table describes the labels in this screen.

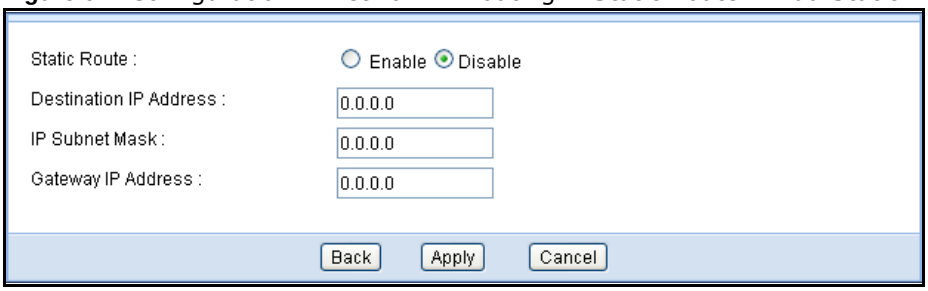
Table 47 Configuration > Network > Routing > Static Route

LABEL	DESCRIPTION
Add Static Route	Click this to create a new rule.
Static Route Rules	
#	This is the index number of an individual static route. The first entry is for the default route and not editable.
Status	This field indicates weather the rule is active (yellow bulb) or not (gray bulb).
Destination	Displays the IP network address of the final destination. Routing is always based on network number.
Gateway	Displays the IP address of the gateway. The gateway is an immediate neighbor of your EMG1302-R10A that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your EMG1302-R10A; over the WAN, the gateway must be the IP address of one of the remote nodes.
Subnet Mask	Displays the subnet to which the route's final destination belongs.
Modify	Click the **Edit** icon to open the static route screen. Modify a static route. Click the **Remove** icon to delete a static route.

14.2.1 Add/Edit Static Route Screen

To add or edit a static route click the **Add Static Route** in **Configuration** > **Network** > **Static Route** > **Static Route** screen or click on Edit icon under Modify in **configuration** > **Network** > **Static Route** > **Static Route**. Fill in or change the required information for each static route.

Figure 67 Configuration > Network > Routing > Static Route > Add Static Route



The following table describes the labels in this screen.

Table 48 Configuration > Network > Routing > Static Route > Add Static Route

LABEL	DESCRIPTION
Static route	This field allows you to enable/disable the static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Netmask	This is the subnet to which the route's final destination belongs.
Gateway IP Address	Enter the IP address of the gateway. This gateways is an immediate neighbor of your EMG1302-R10A that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your EMG1302-R10A; over the WAN, the gateway must be the IP address of one of the Remote Nodes.
Back	Click the **Back** icon to return to the previous page.

Table 48 Configuration > Network > Routing > Static Route > Add Static Route (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

14.3 The Dynamic Routing Screen

Click **Configuration > Network > Routing > Dynamic Routing** to open the **Dynamic Routing** screen.

Figure 68 Configuration > Network > Routing > Dynamic Routing

The following table describes the labels in this screen.

Table 49 Configuration > Network > Routing > Dynamic Routing

LABEL	DESCRIPTION
Dynamic Routing	
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

15

Interface Group

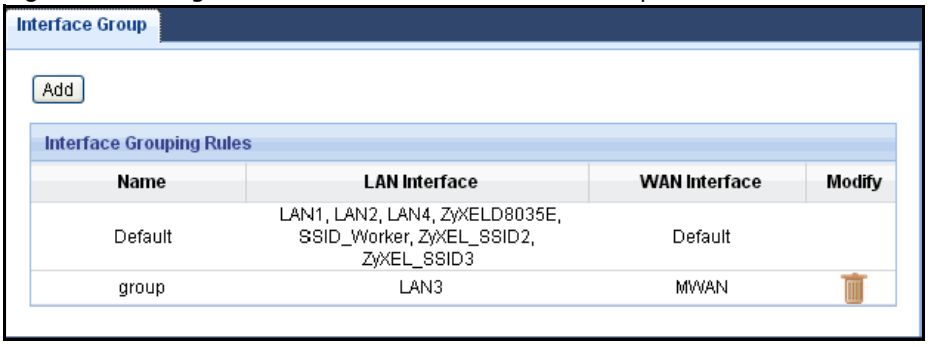
15.1 Overview

By default, all LAN and WAN interfaces on the EMG1302-R10A are in the same group and can communicate with each other. You can create multiple groups to have the EMG1302-R10A assign the IP addresses in different domains to different groups. Each group acts as an independent network on the EMG1302-R10A.

15.2 The Interface Group Screen

You can manually add a LAN interface or a VLAN ID to a new group. Click **Configuration > Network** > **Interface Group** to open the following screen.

Figure 69 Configuration > Network > Interface Group



The following table describes the fields in this screen.

Table 50 Configuration > Network > Interface Group

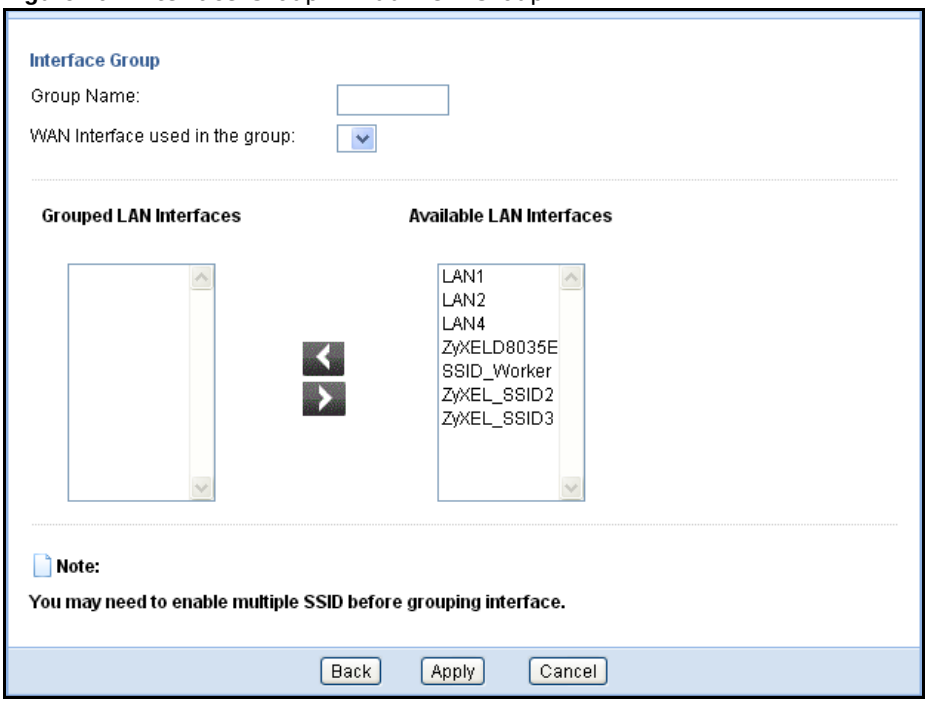
LABEL	DESCRIPTION
Add	Click this to add a new interface grouping rule. You must configure a WAN connection before you can add a new interface grouping rule. See Chapter 7 on page 53 for more information.
Interface Grouping Rules	
Name	This shows the descriptive name of the group.
LAN Interfaces	This shows the LAN interfaces in the group.
WAN Interfaces	This shows the WAN interfaces in the group.
Modify	Select the **Delete** icon to delete the group from the EMG1302-R10A.

15.2.1 Add Interface Group

Click the **Add** button in the **Interface Group** screen to open the following screen. Use this screen to create a new interface group.

Note: An interface can belong to a group only.

Figure 70 Interface Group > Add New Group



The following table describes the fields in this screen.

Table 51 Interface Group > Add New Group

LABEL	DESCRIPTION
Interface Grouping	
Group Name	Enter a name to identify this group.
WAN Interfaces used in the grouping	Select the WAN interface this group uses. The group can have up to one PTM interface and up to one ATM interface.
Grouped LAN Interfaces Available LAN Interfaces	Select a LAN or WAN interface in **Available LAN Interfaces** and use the left-facing arrow to move it to the **Grouped LAN Interfaces** to add the interface to this group. To remove a LAN or WAN interface from the **Grouped LAN Interfaces**, select it and click the right-facing arrow.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

16 Security

16.1 Overview

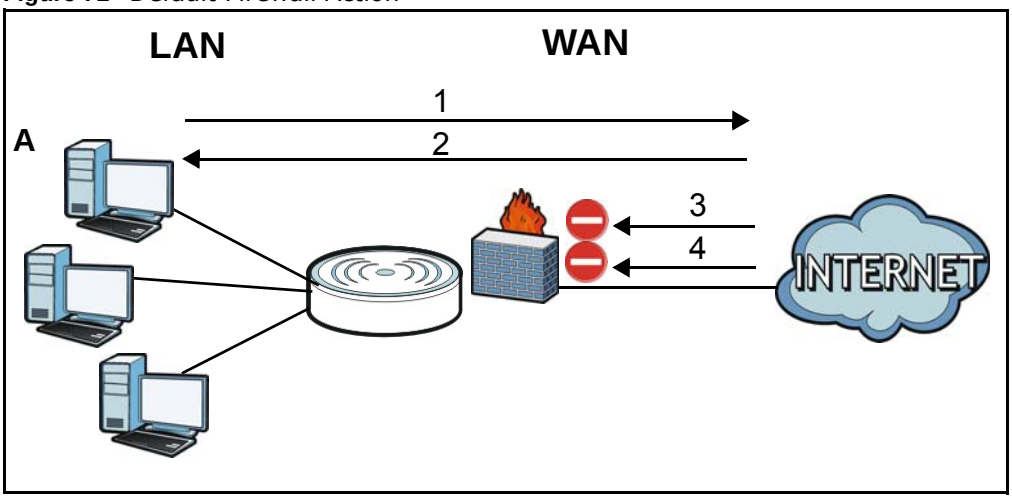
Use these screens to enable and configure the firewall that protects your EMG1302-R10A and your LAN from unwanted or malicious traffic.

Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN and WAN. By default the firewall:

- allows traffic that originates from your LAN computers to go to all of the networks.
- blocks traffic that originates on the other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 71 Default Firewall Action



16.2 What You Can Do

- Use the **General** screen to enable or disable the EMG1302-R10A's firewall (Section 16.4 on page 125).
- Use the **Services** screen to configure the EMG1302-R10A's ICMP settings (Section 16.5 on page 126).

16.3 What You Need To Know

The following terms and concepts may help as you read through this chapter.

What is a Firewall?

Originally, the term “firewall” referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from a network that is not trusted. Of course, firewalls cannot solve every security problem. A firewall is one of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the only mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

Stateful Inspection Firewall

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

About the EMG1302-R10A Firewall

The EMG1302-R10A’s firewall feature physically separates the LAN and the WAN and acts as a secure gateway for all data passing between the networks.

It is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click the **General** tab under **Firewall** and then click the **Enable Firewall** check box). The EMG1302-R10A's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The EMG1302-R10A can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The EMG1302-R10A is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The EMG1302-R10A has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas.The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

Guidelines For Enhancing Security With Your Firewall

1 Change the default password via Web Configurator.

2 Think about access control before you connect to the network in any way, including attaching a modem to the port.

3 Limit who can access your router.

4 Don't enable any local service (such as NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.

5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.

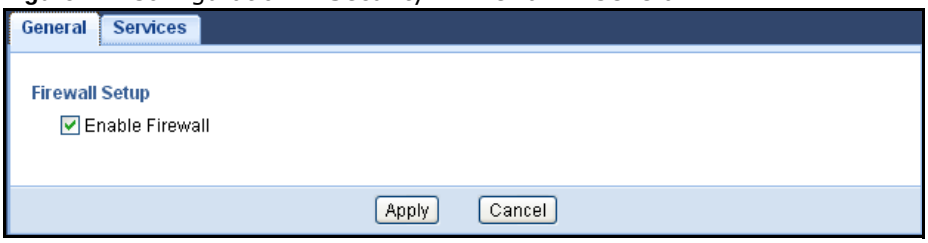
6 Protect against IP spoofing by making sure the firewall is active.

7 Keep the firewall in a secured (locked) room.

16.4 The Firewall General Screen

Use this screen to enable or disable the EMG1302-R10A's firewall, and set up firewall logs. Click **Configuration** > **Security** > **Firewall** to open the **General** screen.

Figure 72 Configuration > Security > Firewall > General l



The following table describes the labels in this screen.

Table 52 Configuration > Security > Firewall > General

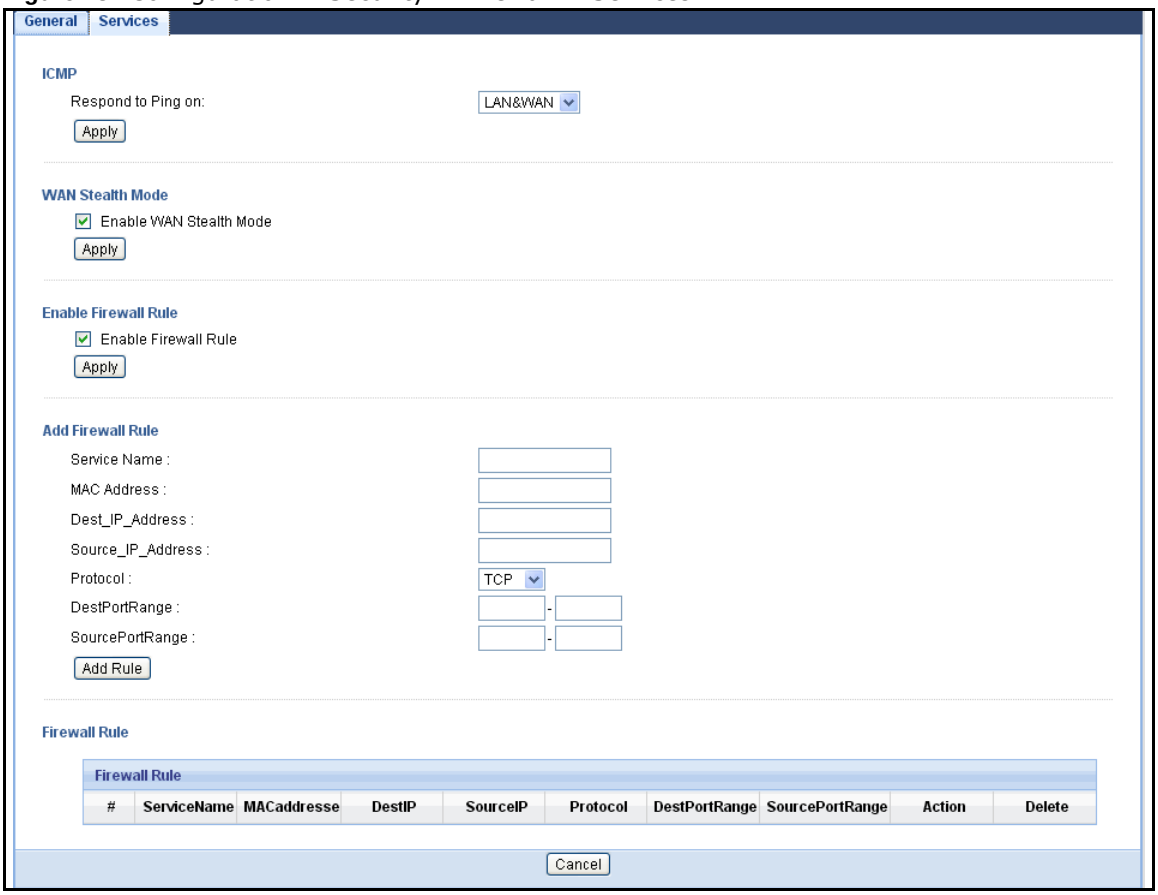
LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The EMG1302-R10A performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to exit this screen without saving.

16.5 The Firewall Services Screen

If an outside user attempts to probe an unsupported port on your EMG1302-R10A, an ICMP response packet is automatically returned. This allows the outside user to know the EMG1302-R10A exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your EMG1302-R10A when unsupported ports are probed.

Click **Configuration** > **Security** > **Firewall** > **Services** to display the following screen.

Figure 73 Configuration > Security > Firewall > Services



The following table describes the labels in this screen.

Table 53 Configuration > Security > Firewall > Services

LABEL	DESCRIPTION
ICMP	
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The EMG1302-R10A will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN & WAN** to reply to all incoming LAN and WAN Ping requests.

Table 53 Configuration > Security > Firewall > Services (continued)

LABEL	DESCRIPTION
WAN Stealth Mode	
Enable WAN Stealth Mode	
Enable Firewall Rule	
Enable Firewall Rule	Select this check box to enable firewall rule and click **Apply**.
Add Firewall Rule	
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.
Dest_IP_Address	Enter the IP address of the computer to which traffic for the application or service is entering. The EMG1302-R10A applies the firewall rule to traffic initiations from this computer.
Source_IP_Address	Enter the IP address of the computer that initializes traffic for the application or service. The EMG1302-R10A applies the firewall rule to traffic initiating from this computer.
Protocol	Select the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
DestPortRange	Enter the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
SourcePortRange	Enter the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Add Rule	Click to add rule.
Firewall Rule	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
ServiceName	This is a name that identifies or describes the firewall rule.
MACaddress	This is the MAC address of the computer for which the firewall rule applies.
DestIP	This is the IP address of the computer to which traffic for the application or service is entering.
SourceIP	This is the IP address of the computer to which traffic for the application or service is initialized.
Protocol	This is the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
DestPortRange	This is the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
SourcePortRange	This is the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Action	**DROP** - Traffic matching the conditions of the firewall rule are stopped.
Delete	Click **Delete** to remove the firewall rule.
Cancel	Click **Cancel** to exit this screen without saving.

See Section on page 199 for commonly used services and port numbers.

17

Content Filtering

17.1 Overview

This chapter provides a brief overview of content filtering using the embedded web GUI.

Internet content filtering allows you to create and enforce Internet access policies tailored to your needs. Content filtering is the ability to block certain web features or specific URL keywords.

17.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

Content Filtering Profiles

Content filtering allows you to block certain web features, such as cookies, and/or block access to specific web sites. For example, you can configure one policy that blocks John Doe's access to arts and entertainment web pages.

A content filtering profile conveniently stores your custom settings for the following features.

Keyword Blocking URL Checking

The EMG1302-R10A checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the domain name is www.zyxel.com.tw.

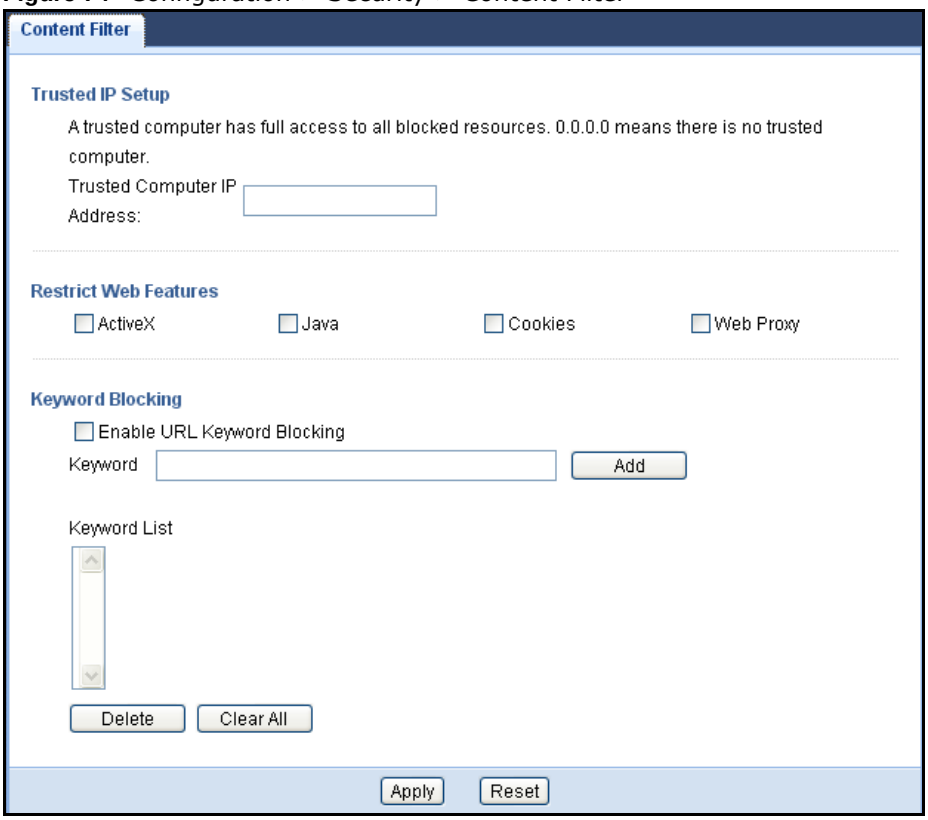
The file path is the characters that come after the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the file path is news/pressroom.php.

Since the EMG1302-R10A checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the EMG1302-R10A would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file path (news/pressroom.php) but it would not find "tw/news".

17.3 Content Filter

Use this screen to restrict web features, add keywords for blocking and designate a trusted computer. Click **Configuration** > **Security** > **Content Filter** to open the **Content Filter** screen.

Figure 74 Configuration > Security > Content Filter



The following table describes the labels in this screen.

Table 54 Configuration > Security > Content Filter

LABEL	DESCRIPTION
Trust IP Setup	
Trusted Computer IP Address	To enable this feature, type an IP address of any one of the computers in your network that you want to have as a trusted computer. This allows the trusted computer to have full access to all features that are configured to be blocked by content filtering. Leave this field blank to have no trusted computers.
Restrict Web Features	
Restrict Web Features	Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.

Table 54 Configuration > Security > Content Filter (continued)

LABEL	DESCRIPTION
Cookies	Used by Web servers to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Keyword Blocking	
Enable URL Keyboard Blocking	The EMG1302-R10A can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be block, e.g., URL http://www.website.com/bad.html would be blocked. Select this check box to enable this feature.
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Add	Click **Add** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Keyword List	This list displays the keywords already added.
Delete	Highlight a keyword in the lower box and click **Delete** to remove it. The keyword disappears from the text box after you click **Apply**.
Clear All	Click **Clear All** to remove all of the listed keywords.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

18

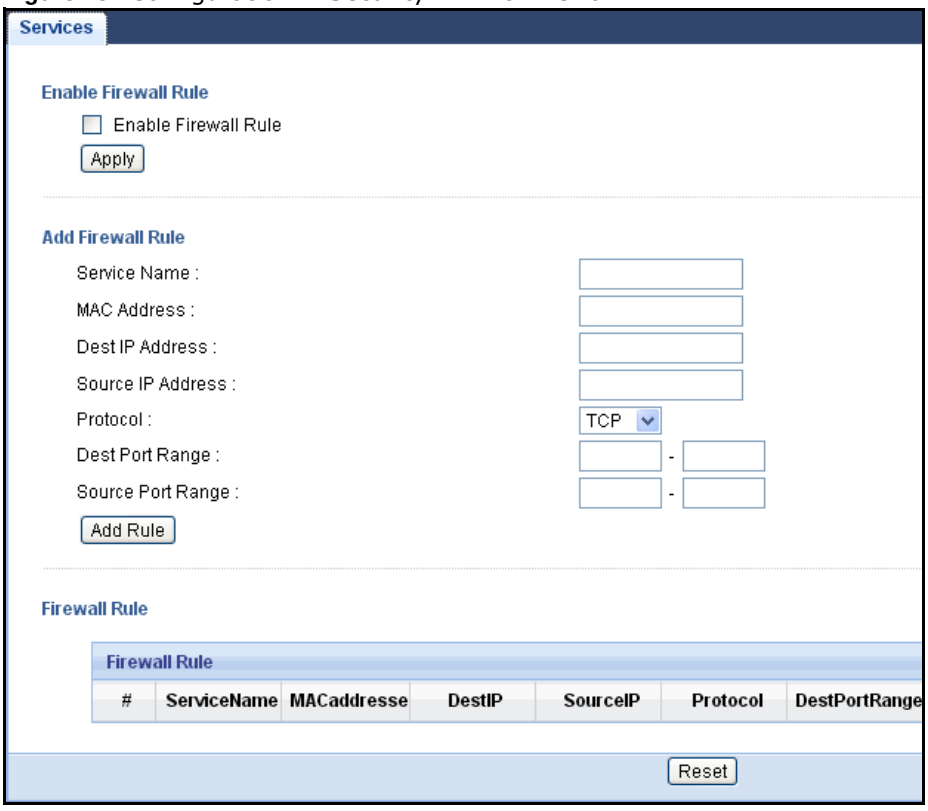
IPv6 Firewall

18.1 Overview

18.2 The IPv6 Firewall Screen

Click **Configuration** > **Security** > **IPv6 Firewall**. The **Service** screen appears as shown.

Figure 75 Configuration > Security > IPv6 Firewall



The following table describes the labels in this screen.

Table 55 Configuration > Security > IPv6 Firewall

LABEL	DESCRIPTION
Enable Firewall Rule	
Enable Firewall Rule	

Table 55 Configuration > Security > IPv6 Firewall (continued)

LABEL	DESCRIPTION
Add Firewall Rule	
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.
Dest IP Address	Enter the IP address of the computer to which traffic for the application or service is entering. The EMG1302-R10A applies the firewall rule to traffic initiations from this computer.
Source IP Address	Enter the IP address of the computer that initializes traffic for the application or service. The EMG1302-R10A applies the firewall rule to traffic initiating from this computer.
Protocol	Select the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	Enter the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	Enter the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Add Rule	Click to add rule.
Firewall Rule	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
ServiceName	This is a name that identifies or describes the firewall rule.
MACaddress	This is the MAC address of the computer for which the firewall rule applies.
DestIP	This is the IP address of the computer to which traffic for the application or service is entering.
SourceIP	This is the IP address of the computer to which traffic for the application or service is initialized.
Protocol	This is the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
DestPortRange	This is the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
SourcePortRange	This is the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Action	**DROP** - Traffic matching the conditions of the firewall rule are stopped.
Delete	Click **Delete** to remove the firewall rule.
Reset	

19

Remote Management

19.1 Overview

This chapter provides information on the Remote Management screens.

Remote Management allows you to manage your EMG1302-R10A from a remote location through the following interfaces:

- LAN and WAN
- LAN only

Note: The EMG1302-R10A is managed using the Web Configurator.

19.2 What You Need to Know

Remote management over LAN or WAN will not work when:

1. The IP address in the **Secured Client IP Address** field (Section 19.4 on page 136) does not match the client IP address. If it does not match, the EMG1302-R10A will disconnect the session immediately.
2. There is already another remote management session. You may only have one remote management session running at one time.
3. There is a firewall rule that blocks it.

19.2.1 Remote Management and NAT

When NAT is enabled:

- Use the EMG1302-R10A's WAN IP address when configuring from the WAN.
- Use the EMG1302-R10A's LAN IP address when configuring from the LAN.

19.3 What You Can Do

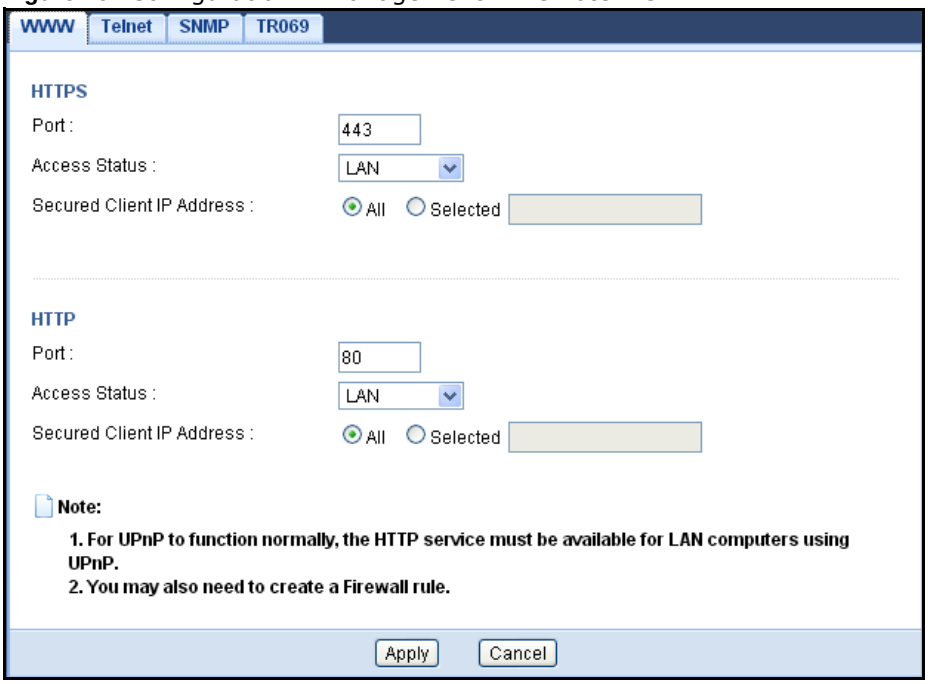
- Use the **WWW** screen to configure through which interface(s) and from which IP address(es) users can use HTTP or HTTPs to manage the NBG4104 (Section 19.4 on page 136).
- Use the **Telnet** screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the EMG1302-R10A (Section 19.5 on page 137).

- Your EMG1302-R10A can act as an SNMP agent, which allows a manager station to manage and monitor the EMG1302-R10A through the network. Use the **SNMP** screen to configure SNMP settings. You can also specify from which IP addresses the access can come (Section 19.6 on page 138).
- Use the **TR069** screen to configure the EMG1302-R10A's TR-069 auto-configuration settings (Section 19.7 on page 140).

19.4 The WWW Screen

To change your EMG1302-R10A's remote management settings, click **Configuration** > **Management** > **Remote MGMT** to open the **WWW** screen.

Figure 76 Configuration > Management > Remote MGMT > WWW



The following table describes the labels in this screen.

Table 56 Configuration > Management > Remote MGMT > WWW

LABEL	DESCRIPTION
HTTPS	
Port	You may change the server port number for a HTTPS service if needed. However you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the EMG1302-R10A using this HTTPS service.
Secured Client IP Address	Select **All** to allow all computers to access the EMG1302-R10A. Otherwise, check **Selected** and specify the IP address of the computer that can access the EMG1302-R10A.
HTTP	
Port	You may change the server port number for a HTTPS service if needed. However you must use the same port number in order to use that service for remote management.

Table 56 Configuration > Management > Remote MGMT > WWW (continued)

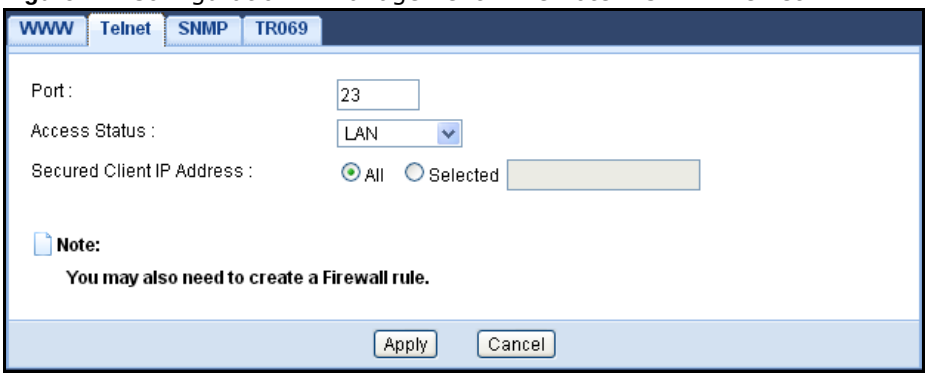
LABEL	DESCRIPTION
Access Status	Select the interface(s) through which a computer may access the EMG1302-R10A using this HTTP service.
Secured Client IP Address	Select **All** to allow all computers to access the EMG1302-R10A. Otherwise, check **Selected** and specify the IP address of the computer that can access the EMG1302-R10A.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

19.5 The Telnet Screen

You can use Telnet to access the EMG1302-R10A's command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

Click **Configuration** > **Management** > **Remote MGMT** > **Telnet** to display the screen as shown.

Figure 77 Configuration > Management > Remote MGMT > Telnet



The following table describes the labels in this screen.

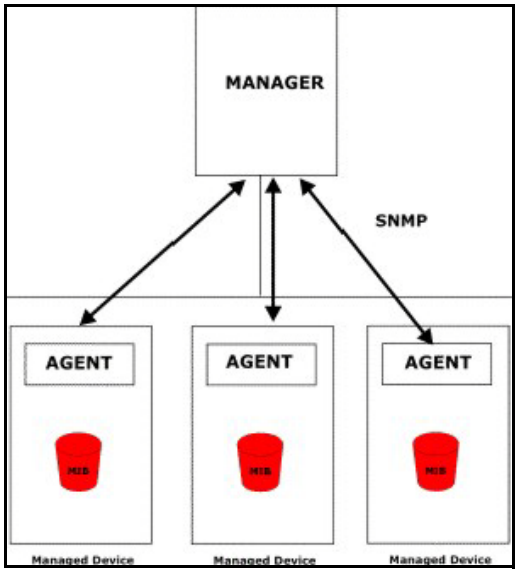
Table 57 Configuration > Management > Remote MGMT > Telnet

LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed. However you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the EMG1302-R10A using this service.
Secured Client IP Address	Select **All** to allow all computers to access the EMG1302-R10A. Otherwise, check **Selected** and specify the IP address of the computer that can access the EMG1302-R10A.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

19.6 The SNMP Screen

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your EMG1302-R10A supports SNMP agent functionality, which allows a manager station to manage and monitor the EMG1302-R10A through the network. The EMG1302-R10A supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 78 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the EMG1302-R10A). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

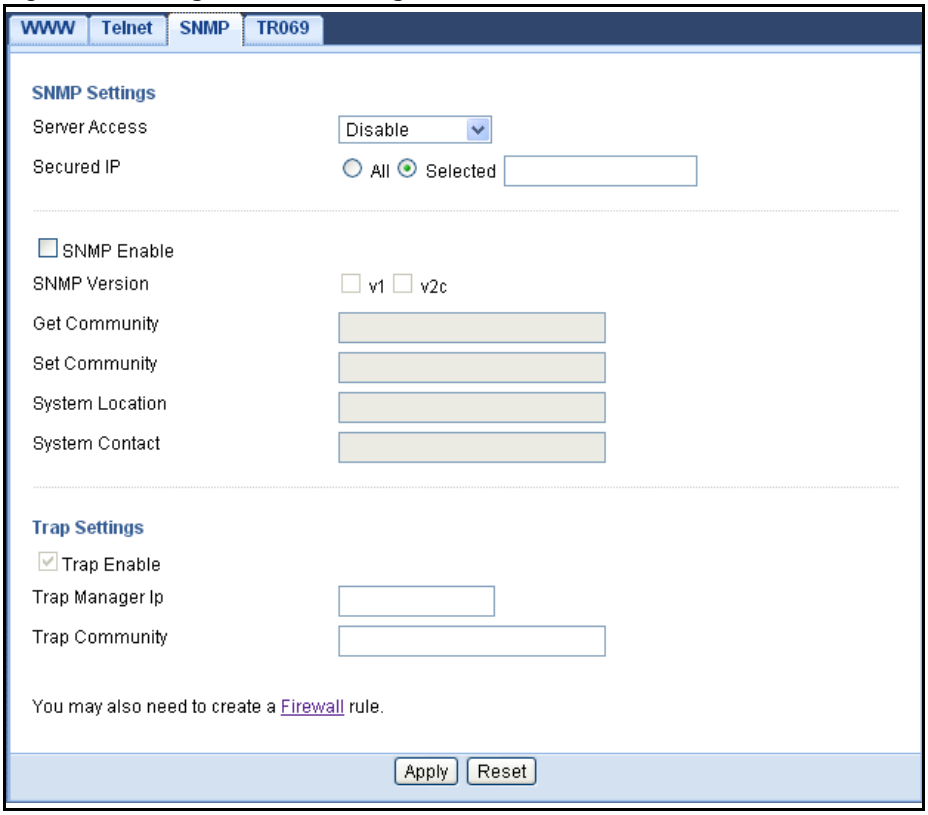
The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

To change your EMG1302-R10A's SNMP settings, click **Configuration** > **Management** > **Remote MGMT** > **SNMP** to display the screen as shown.

Figure 79 Configuration > Management > Remote MGMT > SNMP



The following table describes the labels in this screen.

Table 58 Configuration > Management > Remote MGMT > SNMP

LABEL	DESCRIPTION
SNMP Settings	
Server Access	Select the interface(s) through which a computer may access the EMG1302-R10A using this service.
Secured IP	Select **All** to allow all computers to access the EMG1302-R10A. Otherwise, check **Selected** and specify the IP address of the computer that can access the EMG1302-R10A.
SNMP Enable	Select this to enable SNMP on this device.
SNMP Version	
Get Community	Enter the SNMP get community information here.
Set Community	Enter the SNMP set community information here.
System Location	Enter the SNMP system location.
System Contact	Enter the SNMP system contact.
Trap Settings	
Trap Enable	Select this to enable trap settings on this device.
Trap Manager IP	Type the IP address of the station to send your SNMP traps to.

Table 58 Configuration > Management > Remote MGMT > SNMP (continued)

LABEL	DESCRIPTION
Trap Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

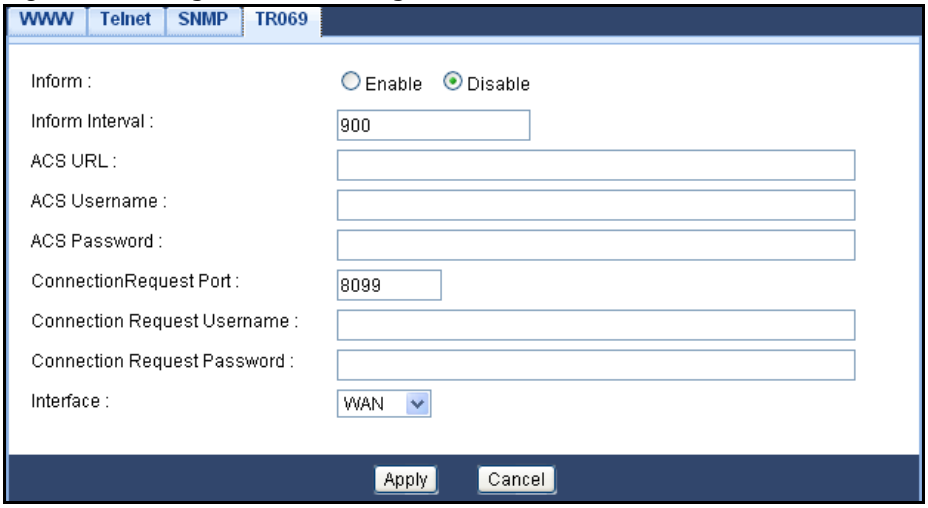
19.7 The TR069 Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your ZyXEL Device, can be managed over the WAN by an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between an ACS and a client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

An administrator can use an ACS to remotely set up the EMG1302-R10A, modify settings, perform firmware upgrades as well as monitor and diagnose the EMG1302-R10A. You have to enable the device to be managed by the ACS and specify the ACS IP address or domain name and username and password.

Click **Configuration** > **Management** > **Remote MGMT** > **TR069** to display the screen as shown. Use this screen to configure your EMG1302-R10A to be managed by an ACS.

Figure 80 Configuration > Management > Remote MGMT > TR069



The following table describes the labels in this screen.

Table 59 Configuration > Management > Remote MGMT > TR069

LABEL	DESCRIPTION
Inform	Select **Enable** for the EMG1302-R10A to send periodic inform via TR-069 on the WAN. Otherwise, select **Disable**.
Inform Interval	Enter the time interval (in seconds) at which the EMG1302-R10A sends information to the auto-configuration server.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS Username	Enter the TR-069 user name for authentication with the auto-configuration server.

Table 59 Configuration > Management > Remote MGMT > TR069 (continued)

LABEL	DESCRIPTION
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
ConnectionRequest Port	
Connection Request Username	Enter the connection request user name. When the ACS makes a connection request to the EMG1302-R10A, this user name is used to authenticate the ACS.
Connection Request Password	Enter the connection request password. When the ACS makes a connection request to the EMG1302-R10A, this password is used to authenticate the ACS.
Interface	Select the network interface.
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

20

Universal Plug-and-Play (UPnP)

20.1 Overview

This chapter introduces the UPnP feature in the web configurator.

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

20.2 What You Need to Know

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

20.2.1 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

20.2.2 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the EMG1302-R10A allows multicast messages on the LAN only.

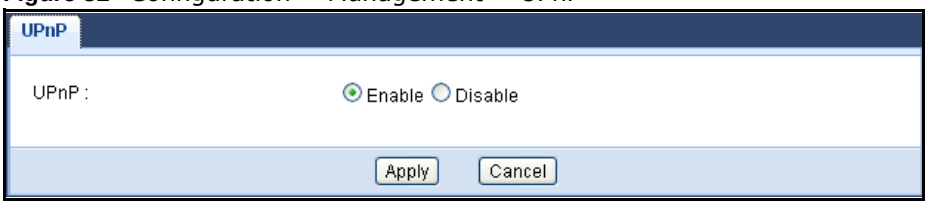
All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

20.3 UPnP Screen

Use this screen to enable UPnP on your EMG1302-R10A.

Click **Configuration** > **Management > UPnP** to display the screen shown next.

Figure 81 Configuration > Management > UPnP



The following table describes the fields in this screen.

Table 60 Configuration > Management > UPnP

LABEL	DESCRIPTION
UPnP	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the EMG1302-R10A's IP address (although you must still enter the password to access the web configurator).
Apply	Click **Apply** to save the setting to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

20.4 Technical Reference

The sections show examples of using UPnP.

20.4.1 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the EMG1302-R10A.

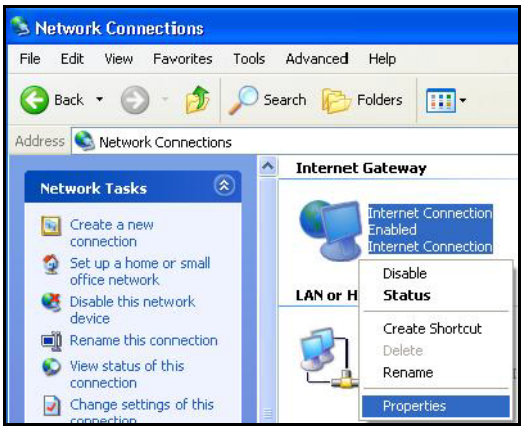
Make sure the computer is connected to a LAN port of the EMG1302-R10A. Turn on your computer and the EMG1302-R10A.

20.4.1.1 Auto-discover Your UPnP-enabled Network Device

1 Click **start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

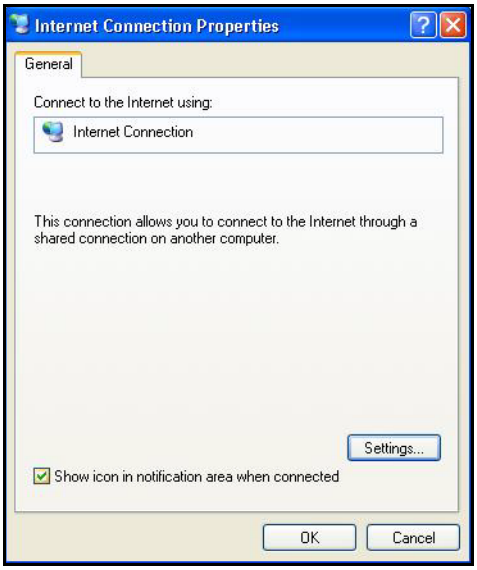
2 Right-click the icon and select **Properties**.

Figure 82 Network Connections



3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 83 Internet Connection Properties


Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 84 Internet Connection Properties: Advanced Settings

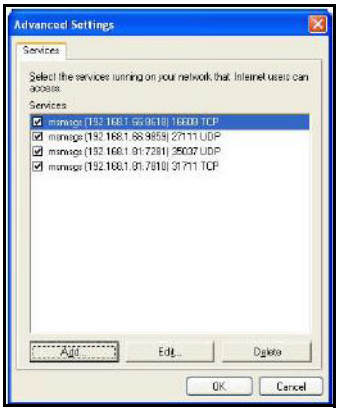
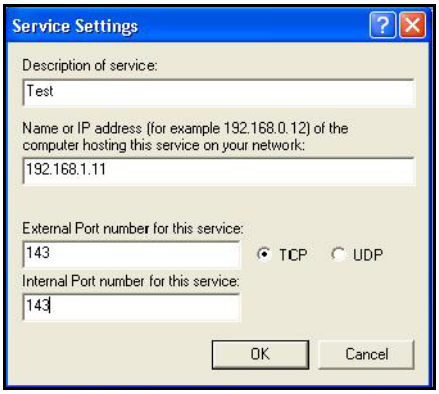


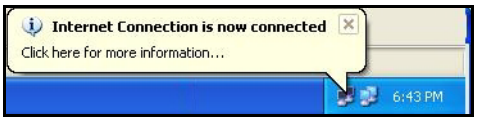
Figure 85 Internet Connection Properties: Advanced Settings: Add



Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

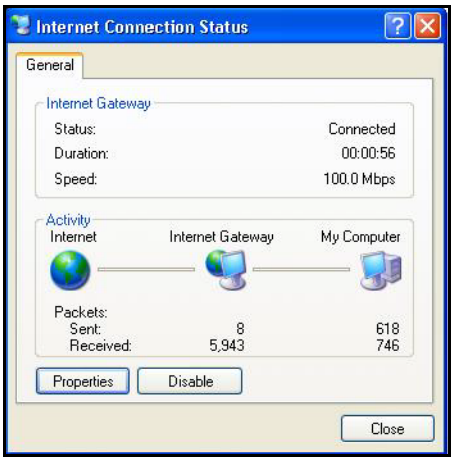
5 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 86 System Tray Icon



6 Double-click on the icon to display your current Internet connection status.

Figure 87 Internet Connection Status



20.4.2 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the EMG1302-R10A without finding out the IP address of the EMG1302-R10A first. This comes helpful if you do not know the IP address of the EMG1302-R10A.

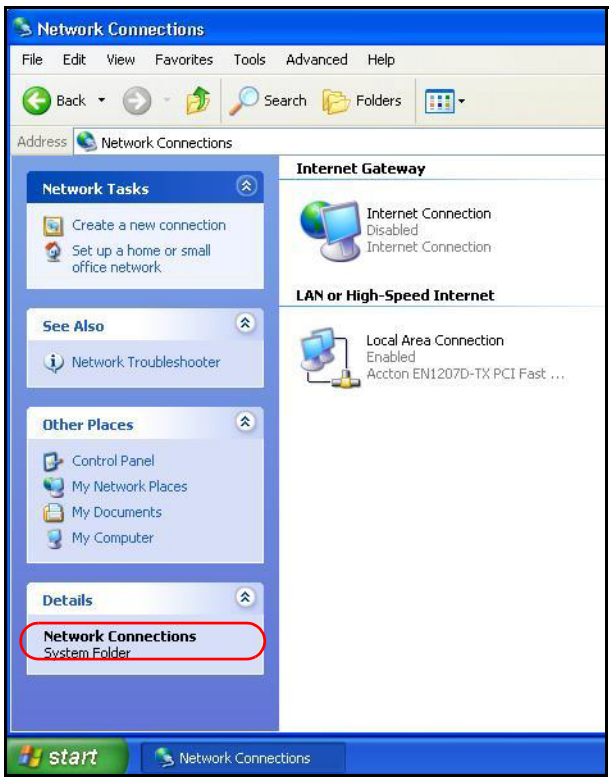
Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

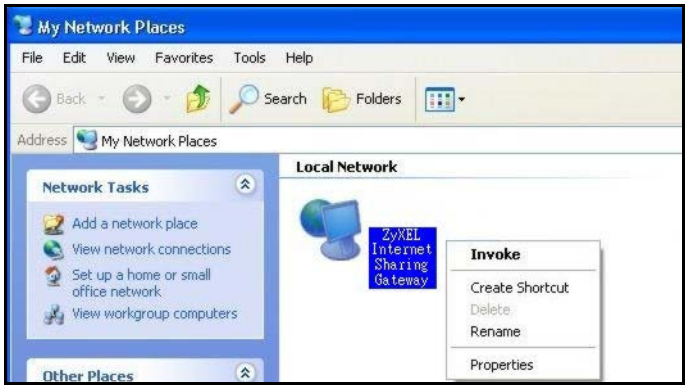
Figure 88 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your EMG1302-R10A and select **Invoke**. The web configurator login screen displays.

Figure 89 Network Connections: My Network Places



6 Right-click on the icon for your EMG1302-R10A and select **Properties**. A properties window displays with basic information about the EMG1302-R10A.

Figure 90 Network Connections: My Network Places: Properties: Example

21 Maintenance

21.1 Overview

This chapter provides information on the **Maintenance** screens.

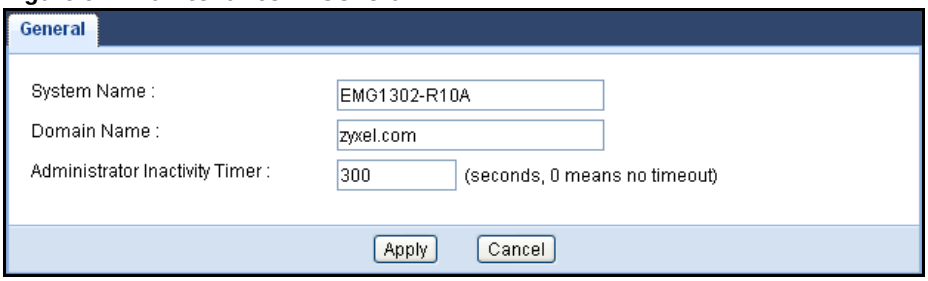
21.2 What You Can Do

- Use the **General** screen to set the timeout period of the management session (Section 21.3 on page 151).
- Use the **Password** screen to change your EMG1302-R10A's system password (Section 21.4 on page 152).
- Use the **Time** screen to change your EMG1302-R10A's time and date (Section 21.5 on page 154).
- Use the **Firmware Upgrade** screen to upload firmware to your EMG1302-R10A (Section 21.6 on page 155).
- Use the **Backup / Restore** screen to view information related to factory defaults, backup configuration, and restoring configuration (Section 21.8 on page 158).
- Use the **Restart** screen to reboot the EMG1302-R10A without turning the power off (Section 21.8 on page 158).

21.3 General Screen

Use this screen to set the management session timeout period. Click **Maintenance** > **General**. The following screen displays.

Figure 91 Maintenance > General



The following table describes the labels in this screen.

Table 61 Maintenance > General

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the EMG1302-R10A in an Ethernet network.
Domain Name	Enter the domain name you want to give to the EMG1302-R10A.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

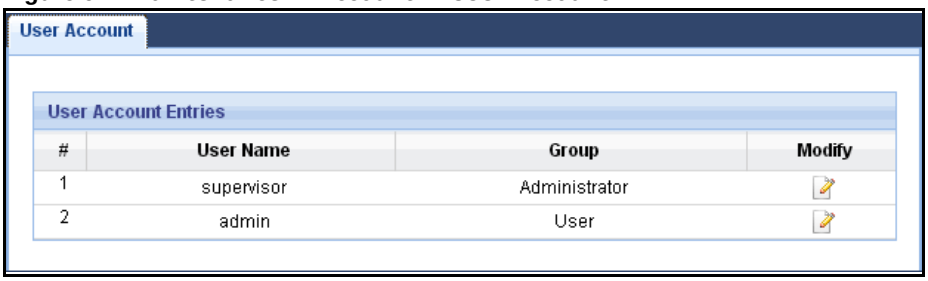
21.4 Account Screen

It is strongly recommended that you change your EMG1302-R10A's password.

If you forget your EMG1302-R10A's password (or IP address), you will need to reset the device. See Section 21.8 on page 158 for details.

Click **Maintenance** > **Account** > **User Account**. The screen appears as shown.

Figure 92 Maintenance > Account > User Account



The following table describes the labels in this screen.

Table 62 Maintenance > Account > User Account

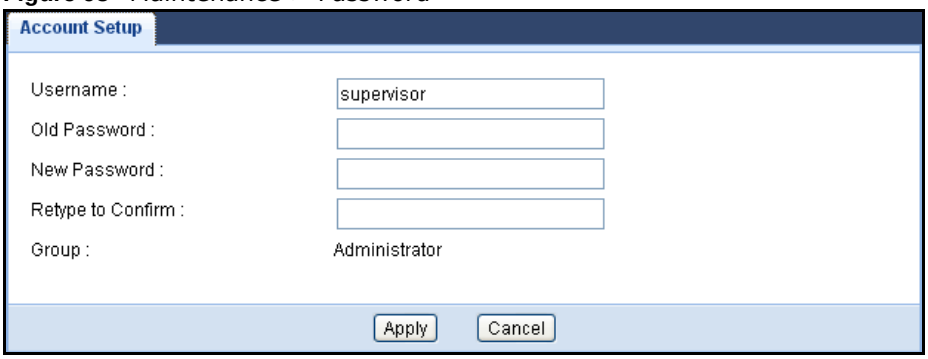
LABEL	DESCRIPTION
User Account Entries	
#	This is the index number of a user account.
User Name	The EMG1302-R10A's user account name.
Group	The belonging of the user account.
Modify	Click the **Edit** icon to open the **Account Setup** screen. Account Setup screen allows to change the user account password.

21.4.1 Account Setup Screen

Account Setup screen allows you to change a user account password.

In User Account Entries in **Maintenance** > **Account** > **User Account**, click **Edit** icon under **Modify**. The screen appears as shown.

Figure 93 Maintenance > Password



The following table describes the labels in this screen.

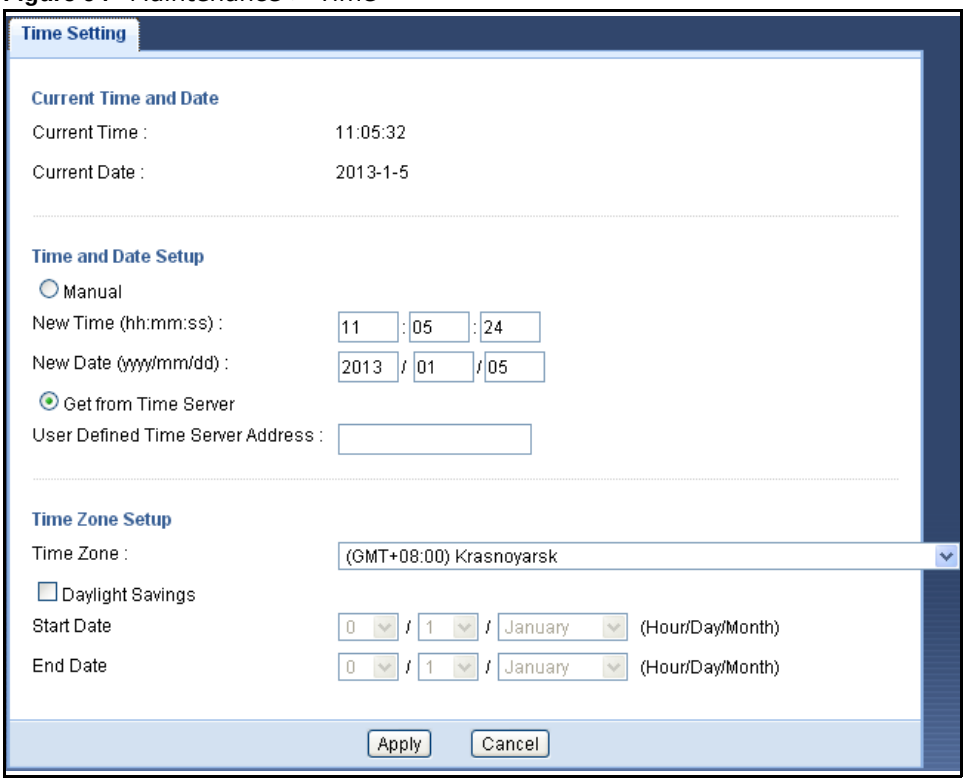
Table 63 Maintenance > Account > User Account > Edit

LABEL	DESCRIPTION
Username	The user account name.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays as asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Group	Shows the group belonging of the user account (read-only).
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

21.5 Time Setting Screen

Use this screen to configure the EMG1302-R10A's time based on your local time zone. To change your EMG1302-R10A's time and date, click **Maintenance** > **Time**. The screen appears as shown.

Figure 94 Maintenance > Time



The following table describes the labels in this screen.

Table 64 Maintenance > Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your EMG1302-R10A. Each time you reload this page, the EMG1302-R10A synchronizes the time with the time server.
Current Date	This field displays the date of your EMG1302-R10A. Each time you reload this page, the EMG1302-R10A synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you select **Manual**, enter the new time in this field and then click **Apply**.

Table 64 Maintenance > Time (continued)

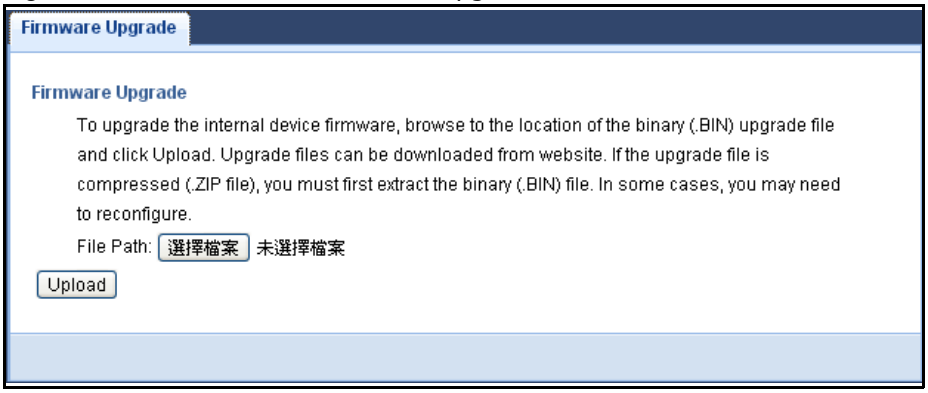
LABEL	DESCRIPTION
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you select **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the EMG1302-R10A get the time and date from the time server you specified below.
User Defined Time Server Address	Select **User Defined Time Server Address** and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples. Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M local time. So in the United States you would select **First**, **Sunday**, **April** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.m. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples. Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Last, Sunday, October** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last, Sunday, October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT + 1).
Apply	Click **Apply** to save your changes back to the EMG1302-R10A.
Cancel	Click **Cancel** to exit this screen without saving.

21.6 Firmware Upgrade Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "EMG1302-R10A.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Maintenance > Firmware Upgrade**. Follow the instructions in this screen to upload firmware to your EMG1302-R10A.

Figure 95 Maintenance > Firmware Upgrade


Firmware Upgrade
Firmware Upgrade
To upgrade the internal device firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure.
File Path:
選擇檔案
未選擇檔案
Upload

The following table describes the labels in this screen.

Table 65 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Firmware Upgrade	
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

Caution: Do not turn off the EMG1302-R10A while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the EMG1302-R10A again.

The EMG1302-R10A automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 96 Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, an error message appears. Click **Return** to go back to the **Firmware Upgrade** screen.

21.7 Configuration Backup/Restore Screen

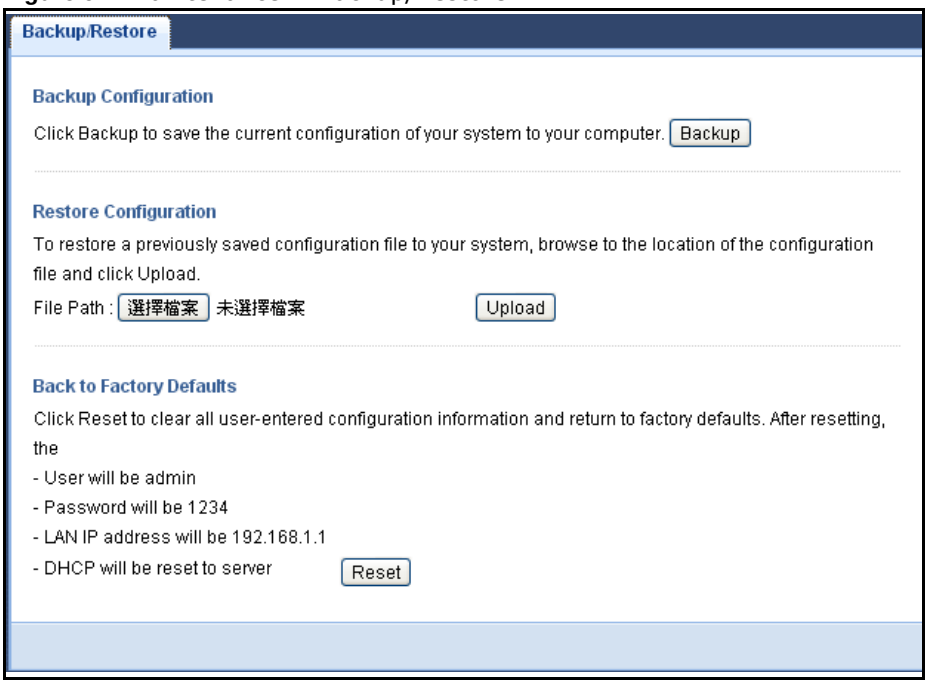
Backup configuration allows you to back up (save) the EMG1302-R10A's current configuration to a file on your computer. Once your EMG1302-R10A is configured and functioning properly, it is highly

recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your EMG1302-R10A.

Click **Maintenance > Backup / Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 97 Maintenance > Backup/Restore


Backup/Restore
Backup Configuration
Click Backup to save the current configuration of your system to your computer.
Backup
Restore Configuration
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.
File Path :
選擇檔案
未選擇檔案
Upload
Back to Factory Defaults
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- User will be admin
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server
Reset

The following table describes the labels in this screen.

Table 66 Maintenance > Backup/Restore

LABEL	DESCRIPTION
Backup Configuration	
Backup	Click **Backup** to save the EMG1302-R10A's current configuration to your computer.
Restore Configuration	
File Path	Click **Choose File** to browse to the location of the configuration file in your computer.

Table 66 Maintenance > Backup/Restore (continued)

LABEL	DESCRIPTION
Upload	Click **Upload** to begin the upload process. Note: Do not turn off the EMG1302-R10A while configuration file upload is in progress. After you see a "configuration upload successful" screen, you must then wait one minute before logging into the EMG1302-R10A again. The EMG1302-R10A automatically restarts in this time causing a temporary network disconnect. If you see an error screen, click Back to return to the Backup/Restore screen.
Reset	Pressing the **Reset** button in this section clears all user-entered configuration information and returns the EMG1302-R10A to its factory defaults. You can also press the **RESET** button on the rear panel to reset the factory defaults of your EMG1302-R10A. Refer to the chapter about introducing the Web Configurator for more information on the **RESET** button.

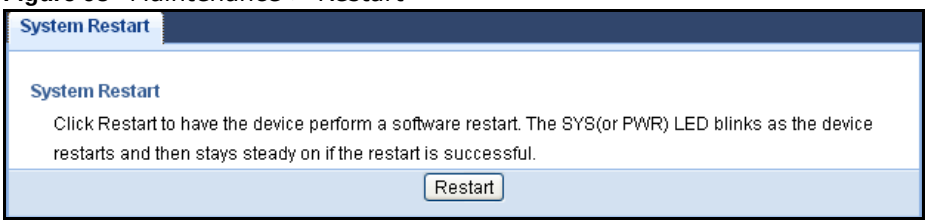
Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default EMG1302-R10A IP address (192.168.1.2). See Appendix C on page 193 for details on how to set up your computer's IP address.

21.8 Restart Screen

System restart allows you to reboot the EMG1302-R10A without turning the power off.

Click **Maintenance > Restart** to open the following screen.

Figure 98 Maintenance > Restart


System Restart
System Restart
Click Restart to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful.
Restart

Click **Restart** to have the EMG1302-R10A reboot. This does not affect the EMG1302-R10A's configuration.

22

Troubleshooting

22.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- EMG1302-R10A Access and Login
- Internet Access
- Resetting the EMG1302-R10A to Its Factory Defaults
- Wireless Router/AP Troubleshooting

22.2 Power, Hardware Connections, and LEDs

The EMG1302-R10A does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the EMG1302-R10A.
2. Make sure the power adaptor or cord is connected to the EMG1302-R10A and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the EMG1302-R10A.
4. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.5 on page 14.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Disconnect and re-connect the power adaptor to the EMG1302-R10A.
5. If the problem continues, contact the vendor.

22.3 EMG1302-R10A Access and Login

I don't know the IP address of my EMG1302-R10A.

1 The default IP address is **192.168.1.1**.

2 If you changed the IP address and have forgotten it, you might get the IP address of the EMG1302-R10A by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the EMG1302-R10A (it depends on the network), so enter this IP address in your Internet browser.Set your device to **Router Mode**, login (see the Quick Start Guide for instructions) and go to the **Device Information** table in the **Status** screen. Your EMG1302-R10A's IP address is available in the **Device Information** table.

- If the **DHCP** setting under **LAN information** is **None**, your device has a fixed IP address.
- If the **DHCP** setting under **LAN information** is **Client**, then your device receives an IP address from a DHCP server on the network.

3 If your EMG1302-R10A is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.

4 Reset your EMG1302-R10A to change all settings back to their default. This means your current settings are lost. See Section 22.5 on page 162 in the **Troubleshooting** for information on resetting your EMG1302-R10A.

I forgot the username and password.

1 The default username is **admin** and password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 22.5 on page 162.

I cannot see or access the **Login** screen in the Web Configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address (Section 9.4 on page 93), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I don't know the IP address of my EMG1302-R10A.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Appendix B on page 173.

4 Make sure your computer is in the same subnet as the EMG1302-R10A. (If you know that there are routers between your computer and the EMG1302-R10A, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Section 9.4 on page 93.
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the EMG1302-R10A. See Section 9.4 on page 93.

5 Reset the device to its factory defaults, and try to access the EMG1302-R10A with the default IP address. See Section 2.4 on page 19.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the EMG1302-R10A using another service, such as Telnet. If you can access the EMG1302-R10A, check the remote management settings and firewall rules to find out why the EMG1302-R10A does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN**/**ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the EMG1302-R10A.

1 Make sure you have entered the password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the Web Configurator while someone is using Telnet to access the EMG1302-R10A. Log out of the EMG1302-R10A in the other session, or ask the person who is logged in to log out.

3 This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.

4 Disconnect and re-connect the power adaptor or cord to the EMG1302-R10A.

5 If this does not work, you have to reset the device to its factory defaults. See Section 22.5 on page 162.

22.4 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
2. If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
3. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
4. Go to **Maintenance** > **Sys OP Mode**. Check your **Configuration Mode** setting.
   - Select **Router Mode** if your device routes traffic between a local network and another network such as the Internet.
   - Select **Access Point** if your device bridges traffic between clients on the same network.
5. If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the EMG1302-R10A), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 14.
2. Reboot the EMG1302-R10A.
3. If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.5 on page 14. If the EMG1302-R10A is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Check the signal strength. If the signal strength is low, try moving the EMG1302-R10A closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
3. Reboot the EMG1302-R10A.
4. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

22.5 Resetting the EMG1302-R10A to Its Factory Defaults

If you reset the EMG1302-R10A, you lose all of the changes you have made. The EMG1302-R10A re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.

You will lose all of your changes when you push the **RESET** button.

To reset the EMG1302-R10A:

1. Make sure the power LED is on.
2. Press the **RESET** button for longer than 1 second to restart/reboot the EMG1302-R10A.
3. Press the **RESET** button for longer than five seconds to set the EMG1302-R10A back to its factory-default configurations.

   If the EMG1302-R10A restarts automatically, wait for the EMG1302-R10A to finish restarting, and log in to the Web Configurator. The password is **1234**.

   If the EMG1302-R10A does not restart automatically, disconnect and reconnect the EMG1302-R10A's power. Then, follow the directions above again.

22.6 Wireless Router/AP Troubleshooting

I cannot access the EMG1302-R10A or ping any computer from the WLAN (wireless AP or router).

1. Make sure the wireless LAN is enabled on the EMG1302-R10A.
2. Make sure the wireless adapter on the wireless station is working properly.
3. Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the EMG1302-R10A.
4. Make sure your computer (with a wireless adapter installed) is within the transmission range of the EMG1302-R10A.
5. Check that both the EMG1302-R10A and your wireless station are using the same wireless and wireless security settings.
6. Make sure traffic between the WLAN and the LAN is not blocked by the firewall on the EMG1302-R10A.
7. Make sure you allow the EMG1302-R10A to be remotely accessed through the WLAN interface. Check your remote management settings.
   - See the chapter on Wireless LAN in the User's Guide for more information.

I set up URL keyword blocking, but I can still access a website that should be blocked.

Make sure that you select the **Enable URL Keyword Blocking** check box in the **Content Filtering** screen. Make sure that the keywords that you type are listed in the **Keyword List**.

I can access the Internet, but I cannot open my network folders.

Make sure your account has access rights to the folder you are trying to open.

I cannot access the Web Configurator after I switched to AP mode.

When you change from router mode to AP mode, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".

Refer to Appendix C on page 193 for instructions on how to change your computer's IP address.

What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.
- Position the antenna for best reception. If the AP is placed on a table or floor, point the antenna upwards. If the AP is placed at a high position, point the antenna downwards. Try pointing the antenna in different directions and check which provides the strongest signal to the wireless clients.

A

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional websites are listed below (see also http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml). Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- ZyXEL Communications Corporation
- http://www.zyxel.com

Asia

China

- ZyXEL Communications (Shanghai) Corp.
  ZyXEL Communications (Beijing) Corp.
  ZyXEL Communications (Tianjin) Corp.
- http://www.zyxel.cn

India

- ZyXEL Technology India Pvt Ltd
- http://www.zyxel.in

Kazakhstan

- ZyXEL Kazakhstan
- http://www.zyxel.kz

Korea

- ZyXEL Korea Corp.
- http://www.zyxel.kr

Malaysia

- ZyXEL Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- ZyXEL Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philipines

- ZyXEL Philippines
- http://www.zyxel.com.ph

Singapore

- ZyXEL Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- ZyXEL Communications Corporation
- http://www.zyxel.com

Thailand

- ZyXEL Thailand Co., Ltd
- http://www.zyxel.co.th

Vietnam

- ZyXEL Communications Corporation-Vietnam Office
- http://www.zyxel.com/vn/vi

Europe

Austria

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

Belarus

- ZyXEL BY
- http://www.zyxel.by

Belgium

- ZyXEL Communications B.V.
- http://www.zyxel.com/be/nl/

Bulgaria

- ZyXEL България
- http://www.zyxel.com/bg/bg/

Czech

- ZyXEL Communications Czech s.r.o
- http://www.zyxel.cz

Denmark

- ZyXEL Communications A/S
- http://www.zyxel.dk

Estonia

- ZyXEL Estonia
- http://www.zyxel.com/ee/et/

Finland

- ZyXEL Communications
- http://www.zyxel.fi

France

- ZyXEL France
- http://www.zyxel.fr

Germany

- ZyXEL Deutschland GmbH
- http://www.zyxel.de

Hungary

- ZyXEL Hungary & SEE
- http://www.zyxel.hu

Latvia

- ZyXEL Latvia
- http://www.zyxel.com/lv/lv/homepage.shtml

Lithuania

- ZyXEL Lithuania
- http://www.zyxel.com/lt/lt/homepage.shtml

Netherlands

- ZyXEL Benelux
- http://www.zyxel.nl

Norway

- ZyXEL Communications
- http://www.zyxel.no

Poland

- ZyXEL Communications Poland
- http://www.zyxel.pl

Romania

- ZyXEL Romania
- http://www.zyxel.com/ro/ro

Russia

- ZyXEL Russia
- http://www.zyxel.ru

Slovakia

- ZyXEL Communications Czech s.r.o. organizacna zlozka
- http://www.zyxel.sk

Spain

- ZyXEL Spain
- http://www.zyxel.es

Sweden

- ZyXEL Communications
- http://www.zyxel.se

Switzerland

- Studerus AG
- http://www.zyxel.ch/

Turkey

- ZyXEL Turkey A.S.
- http://www.zyxel.com.tr

UK

- ZyXEL Communications UK Ltd.
- http://www.zyxel.co.uk

Ukraine

- ZyXEL Ukraine
- http://www.ua.zyxel.com

Latin America

Argentina

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

Ecuador

- ZyXEL Communication Corporation
- http://www.zyxel.com/ec/es/

Middle East

Egypt

- ZyXEL Communication Corporation
- http://www.zyxel.com/homepage.shtml

Middle East

- ZyXEL Communication Corporation
- http://www.zyxel.com/homepage.shtml

North America

USA

- ZyXEL Communications, Inc. - North America Headquarters
- http://www.us.zyxel.com/

Oceania

Australia

- ZyXEL Communications Corporation
- http://www.zyxel.com/au/en/

Africa

South Africa

- Nology (Pty) Ltd.
- http://www.zyxel.co.za

B

Pop-up Windows, JavaScript and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: The screens used below belong to Internet Explorer version 6, 7 and 8. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

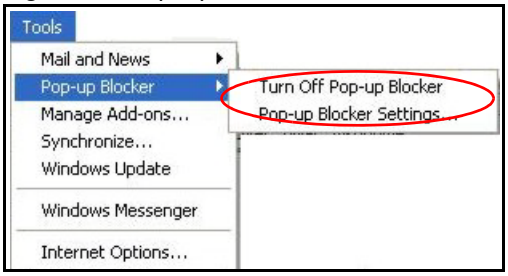
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 99 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 100 Internet Options: Privacy

3 Click **Apply** to save this setting.

Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

Figure 101 Internet Options: Privacy

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 102 Pop-up Blocker Settings

Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Privacy** screen.

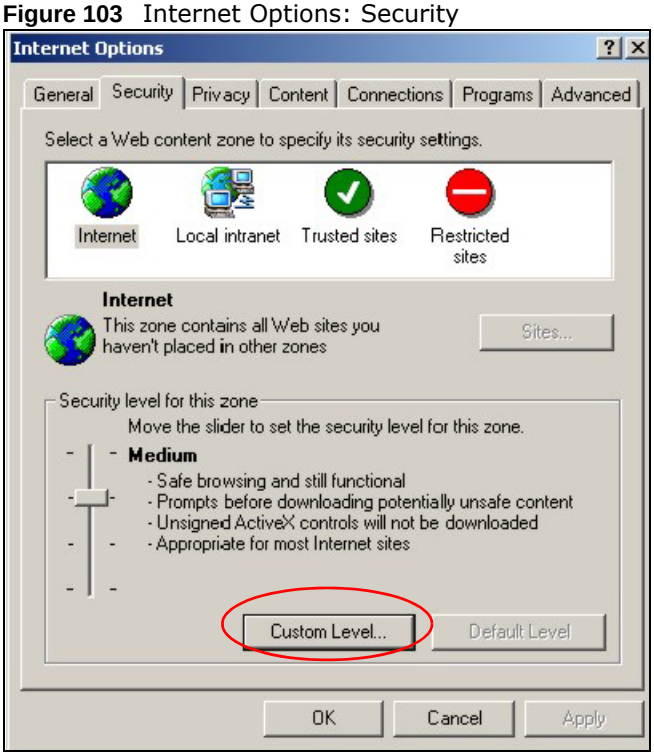
6 Click **Apply** to save this setting.

JavaScript

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScript are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 103 Internet Options: Security



2 Click the **Custom Level...** button.

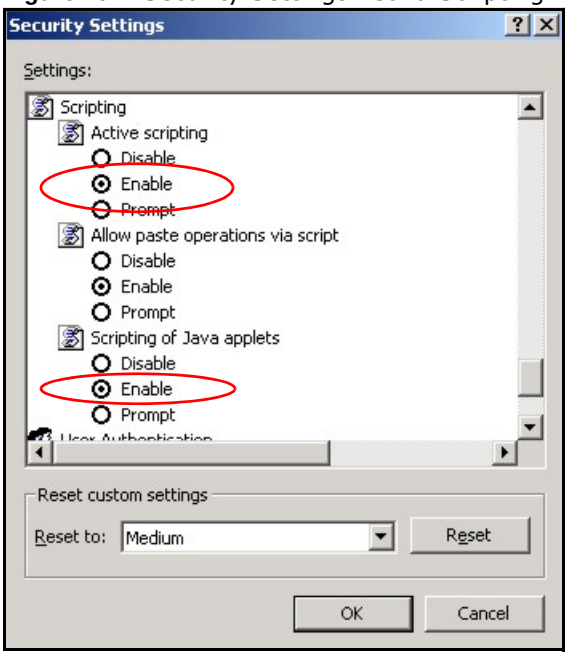
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 104 Security Settings - Java Scripting



Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

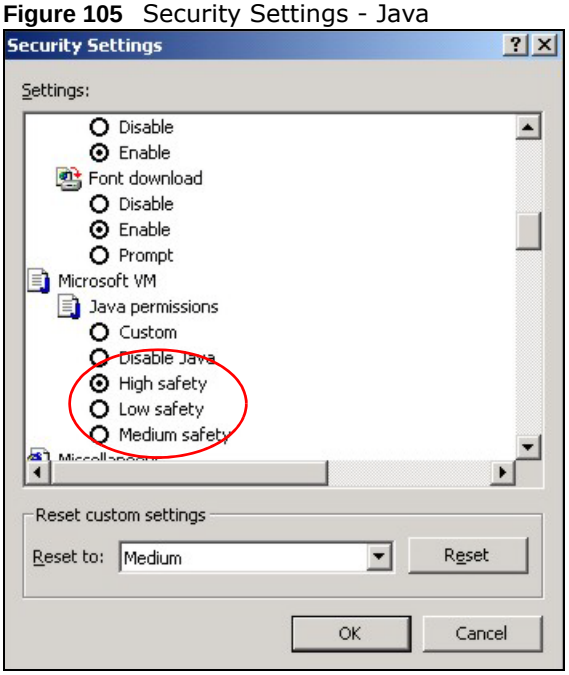
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 105 Security Settings - Java



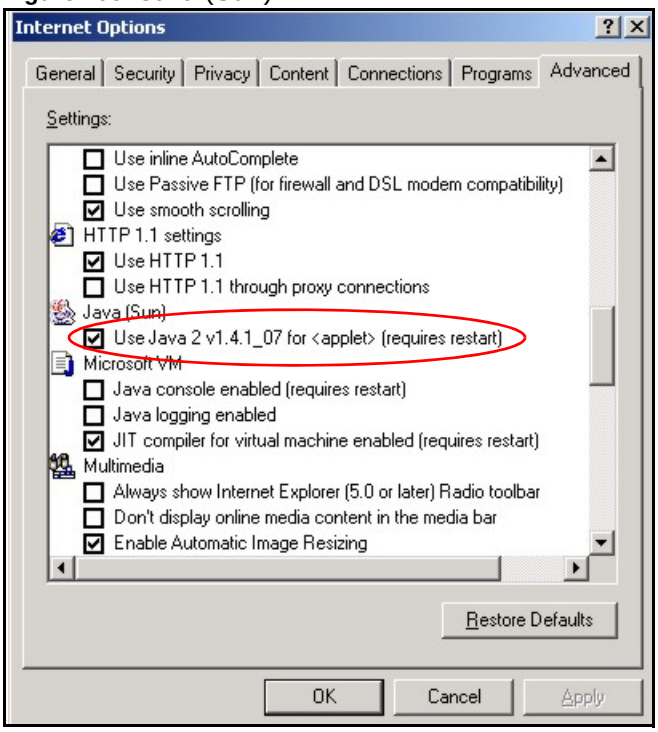
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 106 Java (Sun)

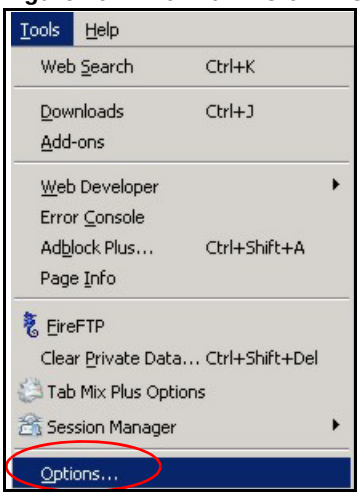


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary slightly. The steps below apply to Mozilla Firefox 3.0 as well.

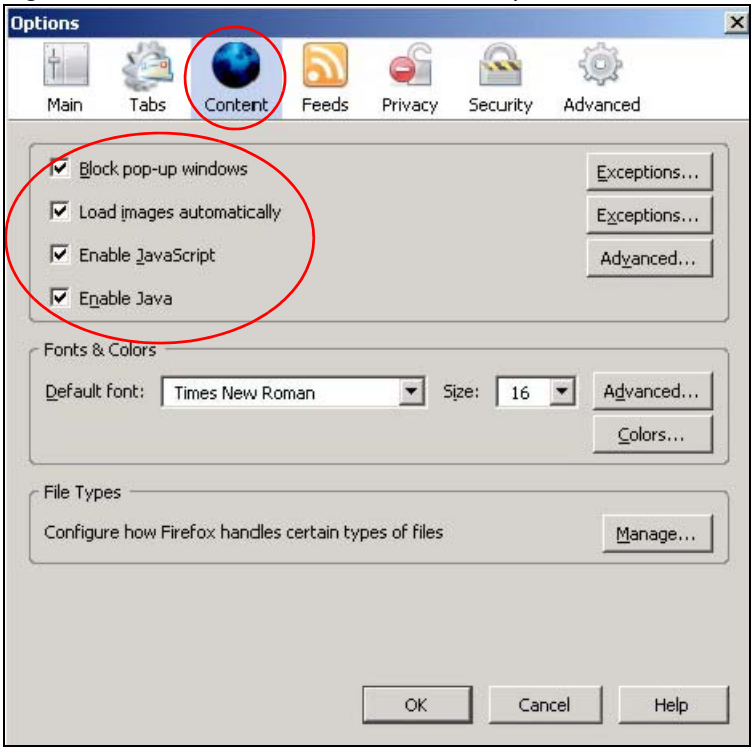
You can enable Java, Javascript and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 107 Mozilla Firefox: TOOLS > Options



Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

Figure 108 Mozilla Firefox Content Security



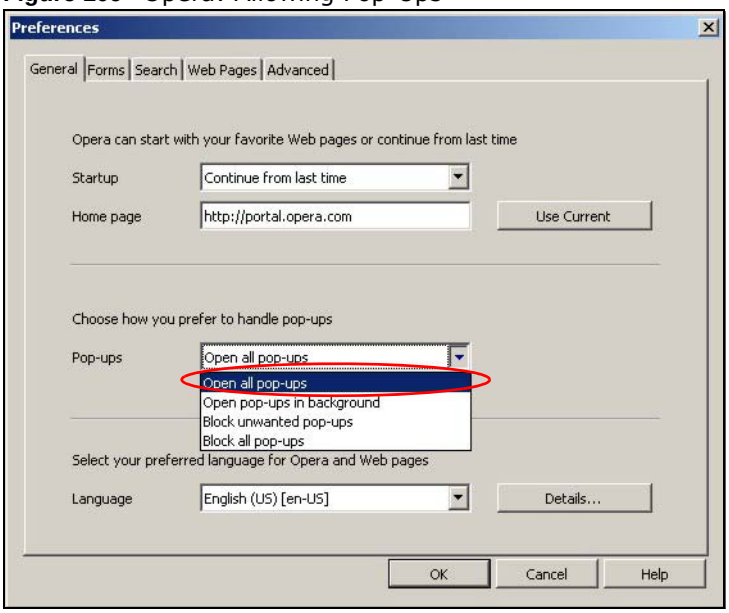
Opera

Opera 10 screens are used here. Screens for other versions may vary slightly.

Allowing Pop-Ups

From Opera, click **Tools**, then **Preferences**. In the **General** tab, go to **Choose how you prefer to handle pop-ups** and select **Open all pop-ups**.

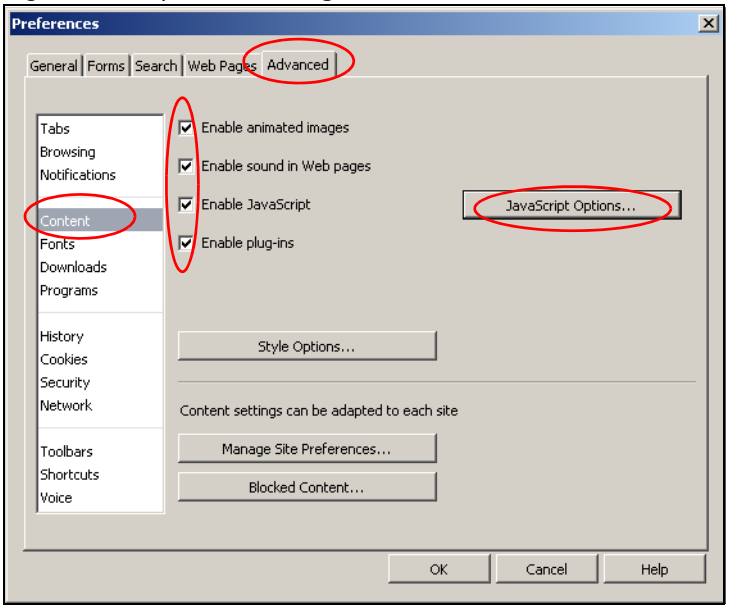
Figure 109 Opera: Allowing Pop-Ups



Enabling Java

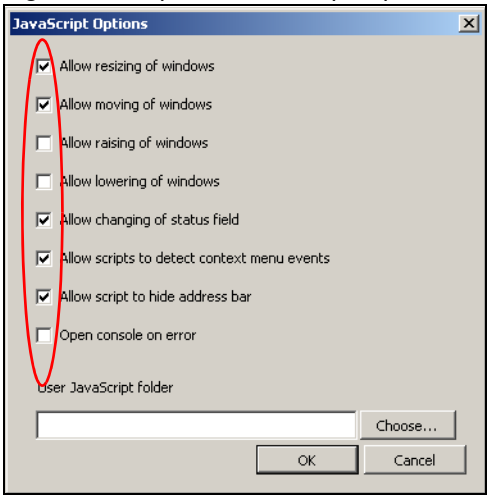
From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 110 Opera: Enabling Java



To customize JavaScript behavior in the Opera browser, click **JavaScript Options**.

Figure 111 Opera: JavaScript Options



Select the items you want Opera's JavaScript to apply.

C

Wireless LANs

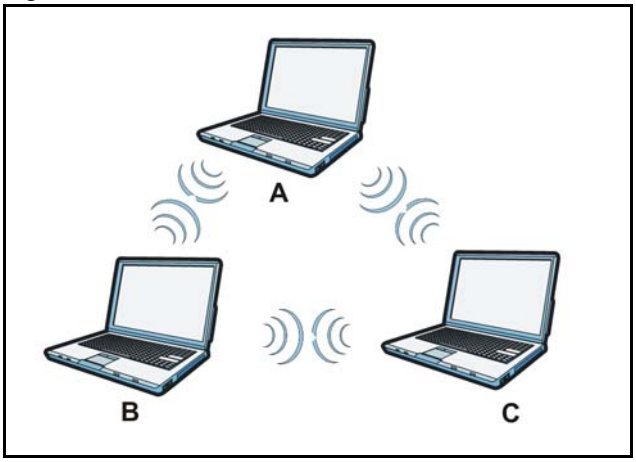
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 112 Peer-to-Peer Communication in an Ad-hoc Network



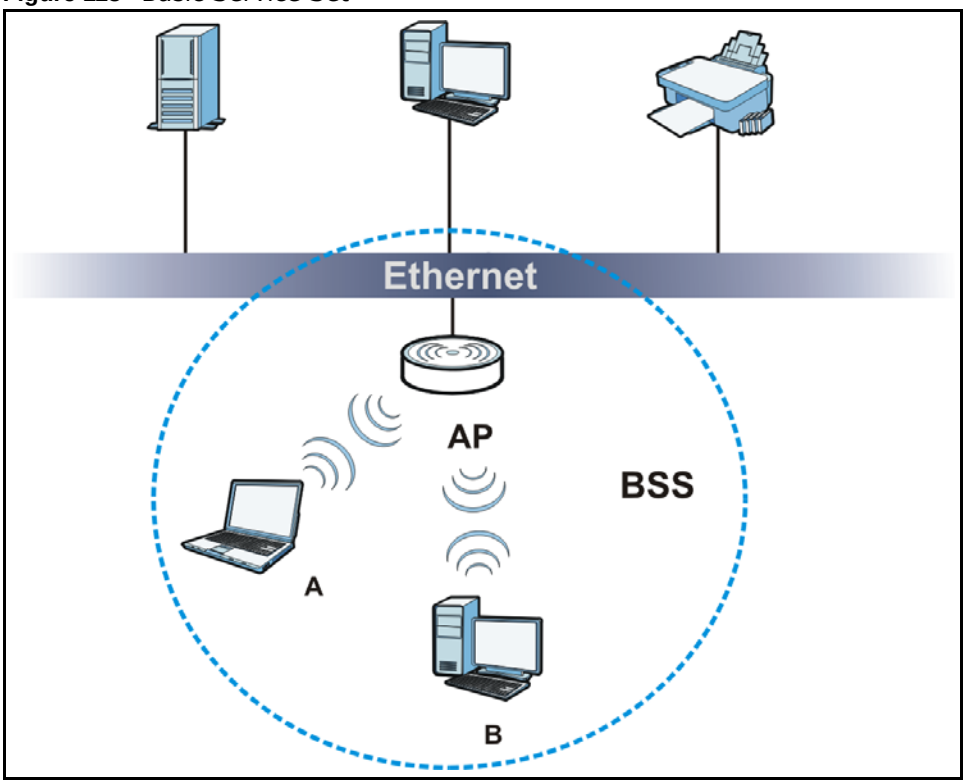
BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is

disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 113 Basic Service Set



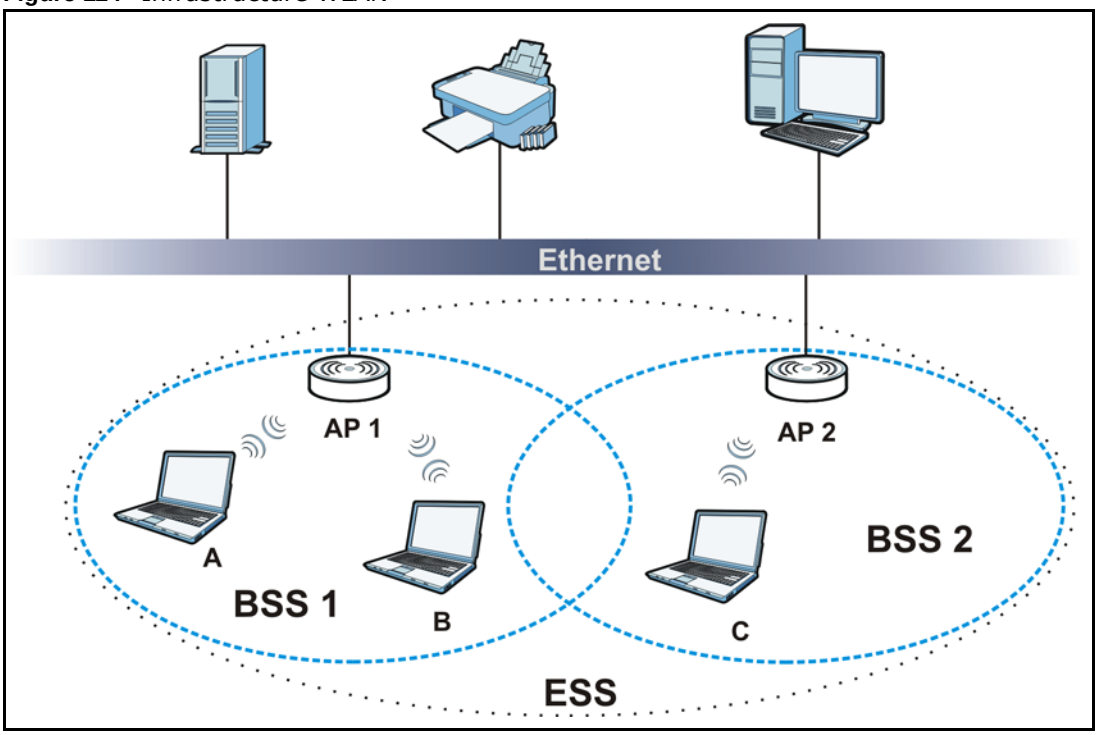
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 114 Infrastructure WLAN



Channel

A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

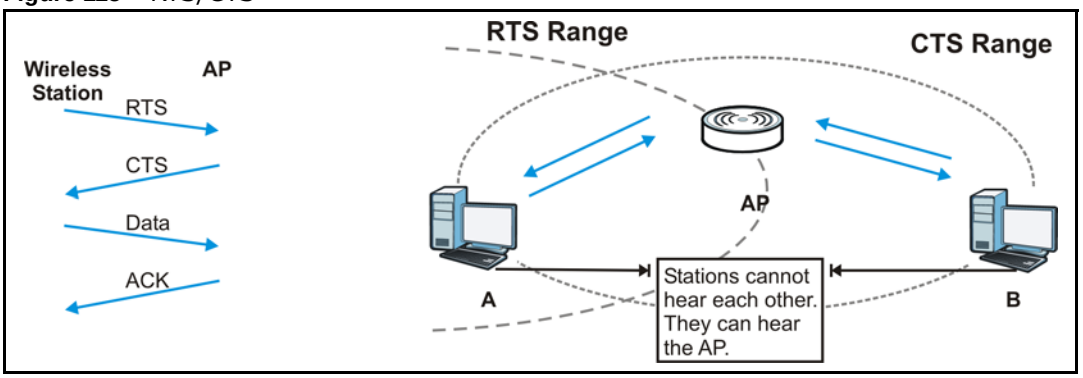
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they

cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 115 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the EMG1302-R10A uses long preamble.

Note: The wireless devices MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 67 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the EMG1302-R10A are data encryption, wireless client authentication, restricting access by device MAC address and hiding the EMG1302-R10A identity.

The following figure shows the relative effectiveness of these wireless security methods available on your EMG1302-R10A.

Table 68 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
	WPA2
Most Secure	

Note: You must enable the same wireless security settings on the EMG1302-R10A and on all wireless clients that you want to associate with it.

IEEE

In June 2001, the IEEE standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client’s network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client ‘proves’ that it knows the password by

encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 69 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

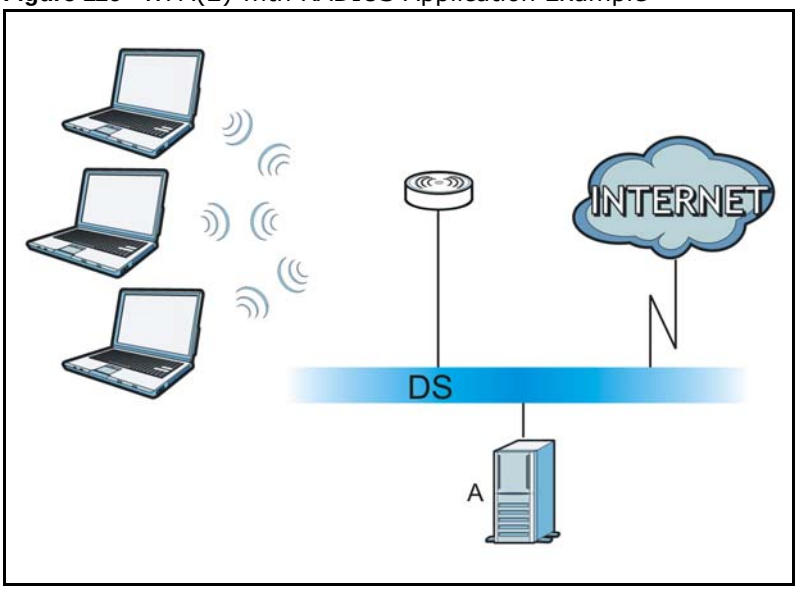
1 The AP passes the wireless client's authentication request to the RADIUS server.

2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

3 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.

4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 116 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

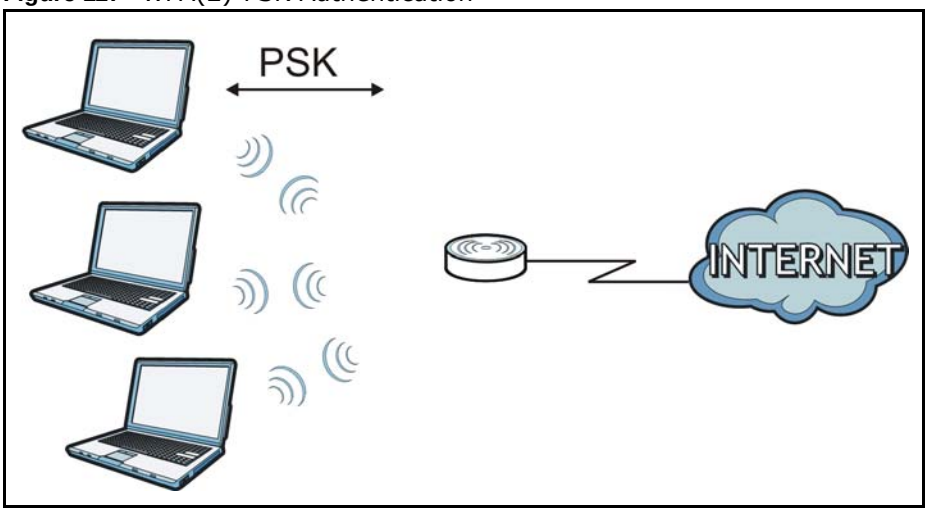
1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

2 The AP checks each wireless client's password and allows it to join the network only if the password matches.

3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 117 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 70 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

D

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 71 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.

Table 71 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
S	TCP	115	Simple File Transfer Protocol.

Table 71 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
T	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

E

Legal Information

Copyright

Copyright © 2013 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Certifications

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1 Reorient or relocate the receiving antenna.
2 Increase the separation between the equipment and the receiver.
3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

4 Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

Note: For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

注意 ！

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package.

You can download the latest firmware at www.zyxel.com. If you cannot find it there, contact your vendor or ZyXEL Technical Support at support@zyxel.com.tw

To obtain the source code covered under those Licenses, please contact your vendor or ZyXEL Technical Support at support@zyxel.com.tw

Regulatory Information

European Union

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

Compliance Information for 2.4GHz and 5GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

[Czech]	ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
[Danish]	Undertegnede ZyXEL erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
[German]	Hiermit erklärt ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
[Estonian]	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, ZyXEL declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
[Spanish]	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
[Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ZyXEL ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕC.
[French]	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
[Italian]	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
[Latvian]	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
[Lithuanian]	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[Dutch]	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
[Maltese]	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
[Hungarian]	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv egyéb elõírásainak.
[Polish]	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
[Portuguese]	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.

[Slovenian]	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
[Slovak]	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
[Finnish]	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[Swedish]	Härmed intygar ZyXEL att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
[Bulgarian]	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/EC.
[Icelandic]	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
[Norwegian]	Erklærer herved ZyXEL at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 1999/5/EF.
[Romanian]	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/EC.

National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2, 4- and 5-GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries inwhich additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for both the 2,4- and 5-GHz wireless LANs.

The following countries have restrictions and/or requirements in addition to those given in the table labeled "*Overview of Regulatory Requirements for Wireless LANs*":.

Overview of Regulatory Requirements for Wireless LANs			
Frequency Band (MHz)	Max Power Level (EIRP)[1] (mW)	Indoor ONLY	Indoor and Outdoor
2400-2483.5	100		V
5150-5350	200	V	
5470-5725	1000		V

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

Denmark

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.

Latvia

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepieciešama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used(specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Malta	MT
Belgium	BE	Netherlands	NL
Cyprus	CY	Poland	PL
Czech Republic	CR	Portugal	PT
Denmark	DK	Slovakia	SK
Estonia	EE	Slovenia	SI
Finland	FI	Spain	ES
France	FR	Sweden	SE
Germany	DE	United Kingdom	GB
Greece	GR	Iceland	IS
Hungary	HU	Liechtenstein	LI
Ireland	IE	Norway	NO
Italy	IT	Switzerland	CH
Latvia	LV	Bulgaria	BG
Lithuania	LT	Romania	RO
Luxembourg	LU	Turkey	TR

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).

- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Index

Numbers

802.1p 105

A

ActiveX 130
Address Assignment 54
Advanced Encryption Standard
  See AES.
AES 193
antenna
  directional 197
  gain 197
  omni-directional 197
AP 13
AP (access point) 187
AP+Bridge 13

B

Basic Service Set, See BSS 185
Bridge/Repeater 13
BSS 185

C

CA 192
Certificate Authority
  See CA.
certifications
  notices 203
  viewing 203
Channel 35
channel 74, 187
  interference 187
Configuration
  restore 157
contact information 166
content filtering 129
  by keyword (in URL) 129
Cookies 131
CPU usage 36
CTS (Clear to Send) 188
customer support 166

D

DDNS
  service providers 115, 119, 133
DHCP 29, 95
  DHCP server
  see also Dynamic Host Configuration Protocol
DHCP server 92, 95
DHCP table 29
  DHCP client information
  DHCP status
disclaimer 203
DNS 97
DNS Server 54
DNS server 97
documentation
  related 2
Domain Name System 97
Domain Name System. See DNS.
duplex setting 36
Dynamic DNS 115
Dynamic Host Configuration Protocol 95
dynamic WEP key exchange 192
DynDNS 115, 119, 133
DynDNS see also DDNS 115, 119, 133

E

EAP Authentication 191
encryption 75, 193
  and local (user) database 76
  key 76
  WPA compatible 76
ESS 186
ESSID 163
Extended Service Set, See ESS 186

F

FCC interference statement 203
Firewall 124
  Firewall overview
  guidelines 125
  network security
  Stateful inspection 124
  ZyXEL device firewall 124
firewall
  stateful inspection 123
Firmware upload 155
  file extension
  using HTTP
firmware version 35
fragmentation threshold 188

G

General wireless LAN screen 76
Guest WLAN 77
Guide
  Quick Start 2

H

hidden node 187

I

IBSS 185
IEEE 802.11g 189
IGMP 55
  see also Internet Group Multicast Protocol
  version
IGMP version 55
Independent Basic Service Set
  See IBSS 185
initialization vector (IV) 193
Interface Group 121
Internet
  wizard setup 21
Internet access
  wizard setup 21
Internet Group Multicast Protocol 55
IP Address 93
IP precedence 105

J

Java 130

L

LAN 91
  IP pool setup 92
LAN overview 91
LAN setup 91
LAN TCP/IP 92
Language 158
Link type 36
local (user) database 75
  and encryption 76
Local Area Network 91

M

MAC 83
MAC address 55, 74

cloning 55
MAC address filter 74
MAC address filtering 83
MAC filter 83
managing the device
good habits 13
using the web configurator. See web configurator.
using the WPS. See WPS.
MBSSID 13
Media access control 83
Memory usage 36
Message Integrity Check (MIC) 193
mode 13
Multicast 55
IGMP 55

N

NAT 107, 110
global 108
how it works 109
inside 108
local 108
outside 108
overview 107
see also Network Address Translation
server 109
NAT Traversal 143
Navigation Panel 37
navigation panel 37
Network Address Translation 107, 110

O

operating mode 13
other documentation 2

P

Pairwise Master Key (PMK) 194, 195
Point-to-Point Protocol over Ethernet 60
port speed 36
PPPoE 60
dial-up connection
preamble mode 189
product registration 205
PSK 194

Q

QoS 101
802.1p 105
example 101
IP precedence 105
priority queue 105
Quality of Service (QoS) 85
Quality of Service, see QoS
Quick Start Guide 2

R

RADIUS 190
message types 191
messages 191
shared secret key 191
RADIUS server 75
registration
product 205
related documentation 2
Remote management
and NAT 135
limitations 135
Reset button 19
Reset the device 19
Restore configuration 157
Roaming 84
Router Mode
status screen 34
RTS (Request To Send) 188
threshold 187, 188
RTS/CTS Threshold 73, 84

S

safety warnings 208
Scheduling 88
Service Set 77, 82
Service Set IDentification 77, 82
Service Set IDentity. See SSID.
SSID 74, 77, 82
stateful inspection firewall 123
Static DHCP 97, 98
Static Route 117
Status 34
Subnet Mask 93
Summary
  DHCP table 29
  Packet statistics 30
  Wireless station status 31
System General Setup 151
System restart 158

T

TCP/IP configuration 95
Temporal Key Integrity Protocol (TKIP) 193
Time setting 154

U

Universal Plug and Play 143
  Application 143
  Security issues 143
UPnP 143
user authentication 75
  local (user) database 75
  RADIUS server 75

W

WAN (Wide Area Network) 53
WAN advanced 70
WAN MAC address 55
warranty 204
  note 204
Web Configurator
  how to access 17
  Overview 17
web configurator 13
Web Proxy 131
WEP Encryption 80
Wi-Fi Protected Access 193
Wireless association list 31
wireless channel 163
wireless client WPA supplicants 194
wireless LAN 163
wireless LAN scheduling 88
Wireless network
  basic guidelines 73
  channel 74
  encryption 75
  example 73
  MAC address filter 74
  overview 73
  security 74
  SSID 74
Wireless security 74
  overview 74
  type 74
wireless security 163, 189
Wireless tutorial 41
wizard setup
  Internet 21
WLAN
  interference 187
  security parameters 196
WPA 193
  key caching 194
  pre-authentication 194
  user authentication 194
  vs WPA-PSK 194
  wireless client supplicant 194
  with RADIUS application example 194
WPA compatible 76
WPA2 193
  user authentication 194
  vs WPA2-PSK 194
  wireless client supplicant 194
  with RADIUS application example 194
WPA2-Pre-Shared Key 193

WPA2-PSK 193, 194
application example 195
WPA-PSK 193, 194
application example 195
WPS 13